UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

MAX STORY and NANCY MURREY-SETTLE,
on behalf of themselves and all others similarly
situated,

                                                   CASE NO.: 3:19-cv-00724-TJC-JBT
                                                   CIVIL DIVISION

        Plaintiffs,

                                                  CLASS REPRESENTATION
v.   **JURY TRIAL DEMANDED**

HEARTLAND PAYMENT SYSTEMS,
LLC, a Foreign Limited Liability Company,

        Defendant.

_____

THIRD AMENDED CLASS ACTION COMPLAINT FOR INJUNCTIVE
RELIEF AND DEMAND FOR JURY TRIAL

      Plaintiffs Max Story and Nancy Murrey-Settle ("Plaintiffs") file this Class Action Complaint on behalf of themselves and all others similarly situated, by and through the undersigned attorneys, against Heartland Payment Systems, LLC (hereinafter "Heartland" or "Defendant"), and state as follows:

I.   INTRODUCTION

      1.   This is a class action on behalf of Plaintiffs and a class of all other similarly situated parents against Heartland Payment Systems, LLC, a credit card payment processing company which owns and operates its MySchoolBucks

Program, which is a stored-value account platform used by over 30,000 schools nationally as a means to provide students with stored value cards that can be used to pay for school meals and other school fees.

2.   Heartland's contractual agreement with parents stated that a "Program Fee" may be required by the school. This statement is false. The "Program Fee" is not a school requirement nor is it a payment for participating in the MySchoolBucks "program." Instead, the "Program Fee" is actually a Credit/Debit Card Surcharge imposed and collected by Heartland, the amount of which is dictated by the payment method used to deposit funds into the child's account.

3.   Parents placing funds into their child's MySchoolBucks account using a credit card are charged a Credit Card Surcharge of approximately $2.49 per transaction.

4.   Parents placing funds into their child's MySchoolBucks account using a debit card are charged a Debit Card Surcharge of approximately $1.95 per transaction.

5.   Because Credit and Debit Card Surcharges are heavily regulated and must be clearly disclosed, Heartland has engaged in an unfair and deceptive practice in violation of New Jersey and Florida law.

II.   JURISDICTION AND VENUE

6.   The Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d), because there are at least 100 Class members in the proposed Class; the combined claims of proposed Class members exceed $5,000,000, exclusive of interest and costs; Plaintiffs are residents of Duval County, Florida; and Defendant conducts an ongoing course of business in Duval County, throughout the State of Florida and the United States.

III.   PARTIES

7.   Plaintiff, Max Story, is a natural person, a resident of Duval County, and a citizen of the State of Florida.

8.   Plaintiff, Nancy Murrey-Settle, is a natural person, a resident of Duval County, and a citizen of the State of Florida.

9.   Defendant, Heartland Payment Systems, LLC, was headquartered in Princeton, New Jersey until it was acquired by Global Payments in April of 2016. Since 2016, Heartland's principal address has been 10 Glenlake Parkway, North Tower, Atlanta, Georgia 30328. Heartland is a corporate citizen of the States of Delaware and Georgia.

IV.   FACTUAL ALLEGATIONS

10.   Heartland Payment Systems, Inc. ("Heartland") is a publicly traded, Fortune 500 Company. It is the fifth largest credit/debit card payment processor in

the United States. It provides credit/debit/prepaid card processing, mobile commerce, e-commerce, and related business services to more than 275,000 business and educational locations nationwide.

11.   When Heartland acts as a credit card payment processor for businesses other than schools, it charges a very small fee to the "merchant" for its services – less than 2%. However, when Heartland processes credit cards for schools, it inflates its rates substantially – often above 5%.

12.   Heartland offers schools across the country its "MySchoolBucks Program" which is the leading K-12 point-of-sale software program that schools use to charge students for items sold at the school, primarily school lunch. The online portal allows parents to deposit funds into their child's MySchoolBucks "account," which acts like a stored-value card similar to a prepaid credit card. By using the MySchoolBucks Program, schools do not have to worry about children carrying cash, staff taking cash, or checks bouncing.

13.   To carry out its MySchoolBucks Program, Heartland enters into a Merchant Agreement with the school district, which makes the school a "merchant" and therefore bound by all the rules imposed on merchants by the credit card companies such as Visa, Mastercard, American Express, and Discover.

14.   Heartland Payment Systems has two separate profit streams generated by its MySchoolBucks Program. First, Heartland charges the school for costs of the

program, including, but not limited to, leasing of equipment including scanners, software, programming, pin pads, training, and maintenance fees. These contracts are automatically renewed and cost substantial amounts each year.

15.   For example, Heartland Payment Systems charged Duval County Public Schools the following amounts over the last five years:

2014 $233,758.99

2015 $99,205.86

2016 $115,786.55

2017 $92,883.75

2018 $86,997.00

2019 $82,167.00

Total $710,799.15

16.   Second, Heartland also charges the school/merchant a Credit/Debit Card Surcharge each time a parent deposits money into a child's MySchoolBucks account. This fee is the same type of fee charged to Heartland's other merchants accepting credit cards, such as retail shops and restaurants. Most of the time, the fees are so low that the merchant simply pays the charge as part of its general overhead. Here, the relationship is different because the merchant/school is *not* the entity taking payment. In other words, the school is not the typical merchant who accepts the credit card from the consumer (parent) and swipes it to access payment. Instead,

Heartland, which is normally just the card processor, steps into the shoes of the merchant/school and accepts payments on behalf of the school/merchant. It then forwards those funds (minus its fee for each transaction) to the school. In other words, Heartland is the payment processor AND the agent of the merchant/school who accepts payment on the school's behalf.

17.   The per transaction fee charged by Heartland for this service is substantially higher than the amounts charged to other merchants. While the school can choose to simply pay Heartland for this service, the inflated rates charged by Heartland would add substantially to the school's overhead. As a result, Heartland offers to "pass through" its Credit/Debit Card Surcharge to parents. The Surcharge, however, is always charged, collected and completely retained entirely by Heartland.

18.   Plaintiffs only learned of this scheme after a Freedom of Information Act request was made to several Florida schools using the MySchoolBucks Program. To understand Heartland's scheme, a brief understanding of its contracts with the schools is required. Because Plaintiffs' children all attend Duval County Public Schools, its contracts are illustrative, although Heartland uses form contracts for schools throughout the country.

A.   **HEARTLAND'S SCHOOL CONTRACTS**

19.   Once the school district has agreed to use the MySchoolBucks Program, Heartland enters into a "K-12 Merchant Processing Agreement" with the school.

Attached hereto as **Exhibit A** is the Merchant Processing Agreement with Duval County Public Schools.

20.   Under the Merchant Processing Agreement, the school becomes the "Merchant" and Heartland, the "Processor."

21.   The Merchant Processing Agreement includes a "Card Fee Schedule" detailing the amounts that Heartland will charge the school each time a credit card or debit card (ACH) is used to place funds into a student's MySchoolBucks account. The Duval County Fee Schedule states as follows:

CARD FEE SCHEDULE

Service Requested	Discount Rate	Discount Per Item	Trans Fee Dial	Trans Fee IP			
Visa	%	$ 2.49			Annual Volume: $ 25,000		Average Ticket: $ 45.00
MasterCard	%	$ 2.49	$ 0	$ 0			High Ticket: $ 45.00
Discover/JCB	%	$ 2.49			☒ Service Fee (Pass Through/Single Transaction)		
TSYS Authorization	%	$	$	$	☐ COST PLUS		
PIN Debit*					*Plus Applicable Debit Network Fees		

Fee Model: ☐ District Absorbed   ☒ Parent Paid

RECURRING FEES / **SETTLEMENT**

Chargeback Fee:	$0	Voice Authorization Fee:	$0	☐Monthly ☒Daily Net

INTERCHANGE QUALIFICATION / **CARD ACCEPTANCE** / **DEPOSIT METHOD**

☒ MOTO / Internet ☐ Retail ☐ Small Ticket	☒ All Cards Accepted	☒ Standard

ACH FEE SCHEDULE

Transaction Fee	$ 1.95	%	Annual ACH Volume: $ 2,500.00	Average ACH Amount: $ 21.00
Monthly Fee		$ 0	Average # of ACH Transactions per Month: 40	
Return Item Fee		$ 0	Max ACH Limit: 500.00	

(**Exhibit A**, Merchant Processing Agreement – Duval County Public Schools).

22.   Heartland charges Duval County Schools a $2.49 Surcharge per credit card transaction, regardless of the amount. For example, a payment of as little as $10 into a MySchoolBucks account will incur a charge of $2.49. This amount far exceeds the amounts Heartland charges its other merchants.

23.   For each transaction in which a debit card (ACH) is used, Heartland imposes a $1.95 Surcharge.

24.   Critically, the "Fee Model" option under the "Card Fee Schedule" gives the school the option of paying these fees itself by checking the "District Absorbed" or Heartland's Credit/Debit Card Surcharge can be passed onto the parent by checking the box labeled "Parent Paid." (**Exhibit A**). On information and belief, thousands of schools across the country elect to have Heartland's Surcharges "passed through" to the parents.

25.   Although there are additional detailed contracts that govern the relationship between the school and Heartland, the Merchant Processing Agreement controls the Credit/Debit Card Surcharges at issue in this case. This document is not publicly available.

26.   Heartland and the school (including Duval County) also enter into another standard-form contract titled "Government and Public Education Credit/Debit Card Processing Agreement." Attached hereto as **Exhibit B** is the Government and Public Education Credit/Debit Card Processing Agreement used by

Duval County Public Schools, and other schools across the country. In that

Agreement, Heartland and the school (collectively the "Merchant") agree to comply

with the rules and regulations of Visa, Mastercard, Discover and American Express

("Credit Card Companies"):

> 4.11. Merchant shall at all times comply with the Rules and operating
> regulations of each of the Card Schemes and American Express as well
> as all applicable federal, state, and local, rules and regulations.

27.   Because Heartland takes credit and debit card payments from parents

on behalf of its school/merchant, Heartland acts as the agent of the merchant/school

and is therefore bound by the Merchant Agreement to follow the rules of the Credit

Card Companies.

28.   Accordingly, the rules and regulations imposed by Visa, Mastercard,

Discover, and American Express, including all requirements for imposing

Credit/Debit Card Surcharges, must be followed by Heartland when acting as the

agent of the merchant/school by collecting payments from parents and charging

Credit/Debit Card Surcharges.

29.   All of the Credit Card Companies require a prominent disclosure of all

Credit/Debit Card Surcharges or Convenience Fees at the point of sale which

explains the nature of the fees, the amount of the fee and how it was calculated. The

Credit Card Companies also limit how much can be charged for such fees. As

explained below, these rules have not been followed by Heartland acting on behalf

of its merchant/school.

30.   Because Heartland's contract states that the Surcharge is actually being

imposed by the merchant/school and is simply being "passed through" to the parent,

Heartland stands in the shoes of the merchant/school as its agent, and is therefore

bound by the rules imposed on merchants by the Credit Card Companies.

31.   Because Heartland fails to disclose the true nature of the Credit/Debit

Card Surcharge at all, it cannot charge these Surcharges without violating the rules

and regulations imposed by the Credit Card Companies. *See generally* **Exhibit C**,

Visa Rules, Section 5.

> **5.6.1.6 US Credit Card Surcharge Maximum Amount – US Region and US Territories**
>
> In the US Region or a US Territory: A US Credit Card Surcharge assessed at the brand level, as specified in *Section 5.6.1.5, US Credit Card Surcharge Requirements – US Region and US Territories*, must not exceed the Merchant's Visa Surcharge Cap.
>
> In the US Region or a US Territory: A US Credit Card Surcharge assessed at the product level, as specified in *Section 5.6.1.5, US Credit Card Surcharge Requirements – US Region and US Territories*, must not exceed the Merchant's Visa Credit Card Surcharge Cap less the Debit Card Cost of Acceptance.
>
> In no case may the US Credit Card Surcharge amount exceed the Maximum Surcharge Cap.
>
> **5.6.1.7 US Credit Card Surcharge Disclosure Requirements – US Region and US Territories**

In the US Region or a US Territory: A Merchant must, at both the point of entry into the Merchant Outlet and the Point-of-Transaction, clearly and prominently disclose any US Credit Card Surcharge that will be assessed.

The disclosure at the Point-of-Transaction must include all of the following:

The exact amount or percentage of the US Credit Card Surcharge

A statement that the US Credit Card Surcharge is being assessed by the Merchant and is only applicable to credit Transactions

A statement that the US Credit Card Surcharge amount is not greater than the applicable Merchant Discount Rate for Visa Credit Card Transactions at the Merchant

Merchants with Acceptance Devices that offer Cardholder choice for debit Transactions in the form of "credit" and "debit" buttons must ensure that:

Debit Card Transactions are not assessed a US Credit Card Surcharge

It is made clear to the Cardholder that surcharges are not permitted on debit Transactions regardless whether a Cardholder selects the "credit" or "debit" button

For an Electronic Commerce Transaction, a Mail/Phone Order Transaction, and an Unattended Transaction, the Cardholder must be provided the opportunity to cancel the Transaction subsequent to the US Credit Card Surcharge disclosure.

For example, the requirement for clear and prominent disclosure will be satisfied if the disclosure is made consistent with *Table 5-5, Surcharge Disclosure – US Region and US Territories*:

Table 5-5: Surcharge Disclosure – US Region and US Territories

Transaction Type	Point-of-Entry	Point-of-Transaction
Face-to-Face Transaction	Main entrance(s) of the Merchant Outlet, in a minimum 32-point Arial font, but in any case no smaller or less prominent than surrounding text	Every customer checkout or payment location, in a minimum 16-point Arial font, but in any case no smaller or less prominent than surrounding text
Electronic Commerce Transaction	The first page that references credit card brands accepted, in a minimum 10-point Arial font, but in any case no smaller or less prominent than surrounding text	Checkout page, in a minimum 10-point Arial font, but in any case no smaller or less prominent than surrounding text
Mail order Transaction	The first page of the catalog that references credit card brands accepted, in a minimum 8-point Arial font, but in any case no smaller or less prominent than surrounding text	Mail order form, in a minimum 10-point Arial font, but in any case no smaller or less prominent than surrounding text
Telephone order Transaction	The first page of the catalog that references credit card brands accepted, in a minimum 8-point Arial font, but in any case no smaller or less prominent than surrounding text	Verbal notice from the telephone order clerk, including US Credit Card Surcharge amount
Unattended Cardholder-Activated Terminal	Main entrance(s) of the Merchant Outlet (if applicable) (for example: gas [petrol] station store) in a minimum 32-point Arial font, but in any case no smaller or less prominent than surrounding text	On the Unattended Cardholder-Activated Terminal or virtual disclosure on the payment terminal screen, in a minimum 16-point Arial font, but in any case no smaller or less prominent than surrounding text

5.6.2.1 Convenience Fees – AP, CEMEA, and US Regions

In the AP Region, CEMEA Region (Russia), US Region: A Merchant that charges a Convenience Fee must ensure that the fee is assessed as follows:

Table 5-6: Convenience Fee Requirements

Convenience Fee Requirement	AP Region	CEMEA Region (Russia)	US Region
Charged for a bona fide convenience in the form of an alternative payment channel outside the Merchant's customary payment channels and not charged solely for the acceptance of a Card	X	X	X
Added only to a Transaction completed in a Card-Absent Environment	X		X
Not charged if the Merchant operates exclusively in a Card-Absent Environment	X		X
Added only to a domestic Unattended Transaction, excluding Transactions at Automated Fuel Dispensers, Telephone Service Transactions, or ATM Cash Disbursements		X	
Charged only by the Merchant that provides goods or services to the Cardholder	X		X
Applicable to all forms of payment accepted in the payment channel	X	X	X
Disclosed clearly to the Cardholder: • As a charge for the alternative payment channel convenience • Before the completion of the Transaction. The Cardholder must be given the opportunity to cancel.	X	X	X
A flat or fixed amount, regardless of the value of the payment due In the AP Region: An ad valorem amount is allowed as required by applicable laws or regulations. In the CEMEA Region (Russia): The amount must not exceed: • RUB 35 for Transactions processed with MCC 4814	X	X	X

13

Table 5-6: Convenience Fee Requirements (continued)

Convenience Fee Requirement	AP Region	CEMEA Region (Russia)	US Region
• RUB 60 for Transactions processed with MCC 4900 • RUB 48 for all other Transactions			
Included as part of the total amount of the Transaction and not collected separately	X	X	X
Not charged in addition to a surcharge	X	N/A[1]	X
Not charged on a Recurring Transaction or an Installment Transaction	X	X	X

[1] Surcharging is not allowed.

32.   Mastercard, Discover, and American Express have similar disclosure requirements before any Surcharge can be charged.

33.   MasterCard Rule 5.11.2.3 governs Requirements for disclosing a surcharge:

5.11.2.3 Requirements for Merchant Disclosure of a Surcharge at the POI

1.   A Merchant that chooses to Surcharge, either at the brand level or the product level, must prominently display a clear disclosure of the Merchant's Surcharge policy at the point of store entry or when conducting an e-commerce Transaction, on the first page that references Credit Card brands. The disclosure must include a statement that the Surcharge that the Merchant imposes is not greater than the Merchant's Merchant Discount Rate for Mastercard Credit Card Transactions.

2.   The Merchant must provide a disclosure of the Merchant's Surcharging practices at the POI or point of sale and that disclosure must not disparage the brand, network, Issuer, or payment card product being used. A statement that the Merchant prefers or requests that a cardholder use a form of payment with

14

lower acceptance costs does not constitute disparagement under this Rule. This disclosure must include:

    a.   The Surcharge percentage that is applied to Mastercard Credit Card Transactions;

    b.   A statement that the Surcharge is being imposed by the Merchant; and

    c.   A statement that the Surcharge is not greater than the applicable Merchant Discount Rate for Mastercard Credit Card Transactions at the Merchant.

3.   A Merchant that chooses to Surcharge must provide clear disclosure of the Surcharge amount on the Transaction receipt.

Mastercard Rule 5.11.2.3, Effective: 27 January 2013 – 6 June 2019.

34.   Because Heartland failed to disclose that its "Program Fee" was actually a Credit/Debit Card Surcharge and/or Convenience Fee, the fees collected by Heartland from parents are strictly prohibited under the rules of all Credit Card Companies. As a result of its failure to follow the rules imposed by the Credit Card Companies, all Surcharges imposed and collected by Heartland are unlawful.

B.   HEARTLAND'S CONTRACT WITH PARENTS

35.   Once the school contracts with Heartland to become a merchant, parents of that school receive notice and are strongly encouraged to use the Heartland system for all payments made to the school. Parents are directed to Heartland's website – www.myschoolbucks.com - to create an account.

36.   The standard form MySchoolBucks Terms of Service Agreement is a contract only between Heartland and parents, like Plaintiffs. The school is not a party to this Agreement. Thus, to the extent that Heartland passes on a charge from the school to the parent, it does so as the agent of the school.

37.   The Agreement in place at the time Plaintiffs were charged Program Fees by Heartland explained the limited service that Heartland was offering, in part, as follows:

> **License and Site Access**
> Heartland Payment Systems, Inc. grants you a limited license to access and make personal use of this Service to pay your child's school for goods and services sold by the school and/or school district (i.e., school meals). You may also be able to use the Service to obtain information about the balance of meal prepayments at your child's school, and to review your child's food purchases at the school cafeteria. …
>
> **Payments to Schools**
> You may make payments to your child's school account by using a credit card. Your credit card provider may have imposed a maximum amount which can be placed on your credit card. **Your child's school receives the full payment.** Payments are processed promptly for your child's use. …
>
> **One Time Payments**
> You authorize MySchoolBucks to debit the bank account indicated in this web form for the noted amount on today's date. You understand that because this is an electronic transaction, these funds may be withdrawn from your account as soon as the above noted transaction date. You acknowledge that the origination of ACH transactions to your account must comply with the provisions of U.S. law.

16

…

Recurring Payments
You authorize MySchoolBucks to debit the bank account indicated in this web form for the noted amount on the schedule indicated. You understand that this authorization will remain in effect until the scheduled end date, or until you cancel the payment, whichever comes first. If the above noted payment falls on a weekend or holiday, you understand that the payment may be executed on the next business day. You understand that because this is an electronic transaction, these funds may be withdrawn from your account as soon as the above noted transaction date. You acknowledge that the origination of ACH transactions to your account must comply with the provisions of U.S. law. …

…

Program Fee or Membership Fee
Your school district may require a program fee or membership fee for your use of the Service.

If you are required to pay a program fee, you will be notified on a screen prior to completing the payment transaction and any such program fee will be required for each payment you make using the Service.

…

Applicable Law
By visiting MySchoolBucks.com, you agree that the laws of the State of New Jersey will govern these Terms of Use, and any dispute relating to the Service provided herein shall be subject to the jurisdiction of the courts of the State of New Jersey.

Exhibit D, MySchoolBucks Terms and Conditions (emphasis added).

38.   Heartland's MySchoolBucks website further clarifies on its Frequently

Asked Questions page the Program Fee as follows:

Is there a fee for using MySchoolBucks?

Signing up for MySchoolBucks is free. Depending on your
school/district and order/item you are purchasing, you may be required
to pay a program or membership fee.

MySchoolBucks Frequently Asked Questions.[1]

39.   Although Heartland's Terms of Service specifically references credit

and debit card payments, it fails to disclose the Credit/Debit Card Surcharges that

are imposed as a result of the Merchant Agreement with the school. In fact,

Heartland's MySchoolBucks Terms and Conditions falsely states that "Your child's

school receives the full payment." (**Exhibit D**, "Payment to Schools").

40.   In fact, the only fee even mentioned by Heartland's Agreement with

parents is the "Program Fee" or "Membership Fee." The explanation of the

"Program Fee" or "Membership Fee" is false and deceptive in three ways.

41.   First, the Program Fee is not accurately explained. The Program Fees

are not charged by the school for participating in the MySchoolBucks "Program."

Instead, they are Credit/Debit Card Surcharges imposed by Heartland under its

Merchant Agreement with the school and "passed through" to the parents under the

terms of that contract. The Surcharges are imposed by Heartland and calculated

---

[1] https://www.myschoolbucks.com/ver2/help/gethelp Site last visited December 4, 2019.

based entirely on the method of payment used. If the fees were not linked to the method of payment, they would not differ when a payment is made with a debit card ($1.95) versus a credit card ($2.49). Similarly, they are only charged when the school and Heartland's Merchant Agreement states that the fees are to be "passed through" to the parents.

42.   Furthermore, Credit/Debit Card Surcharges must be clearly disclosed so that consumers know what they are being charged for, and can inquire of their card provider or bank regarding the legitimacy of the Surcharges. All credit card companies, including Visa, Mastercard, Discover and American Express have specific rules regulating how Credit Card Surcharges can be imposed, including limits on the amount and how notice must be provided to both the Credit Card Company and the consumer. Heartland's Merchant Agreement requires compliance with the Rules established by all Credit Card Companies. Because all Card Providers require clear disclosure of any Credit Card Surcharges, Heartland's "Program Fee" or "Membership Fee" explanation fails to meet any of those requirements and is therefore unfair and deceptive.

43.   Second, the explanation of the Surcharge is false and deceptive because the Credit/Debit Card Surcharges are imposed and collected entirely by Heartland under the credit card and ACH "Fee Schedules" in the Merchant Agreement. In fact,

19

the Merchant Agreement even states that the Surcharges are a "pass through" to Heartland as opposed to a fee imposed by the school.

44.   Third, the Credit/Debit Card Surcharges collected under the guise of "Program" or "Membership" fees, does not go to the school. Instead, these amounts are charged and retained exclusively by Heartland. Under the "Payments to Schools" section of the Terms and Conditions (**Exhibit D**), Heartland states: "Your child's school receives the full payment." When this contract language is combined with the "Program/Membership Fee" explanation that the fee is "required" by the school, a reasonable consumer would believe that the school is receiving all of these amounts. In fact, the entire Credit/Debit Card Surcharge is collected and retained by Heartland.

45.   Some school districts around the country have even attempted to clarify the misleading nature of the representations surrounding the "Program Fees" by issuing precise statements to the public explaining that it is Defendant, and not the school district, which sets and retains the fees. For example, the Souderton Area School District in Pennsylvania released the following notice in regards to the 2017 MySchoolBucks Program Fee increase: "Souderton Area School District does not

collect or receive this fee. It is the fee charged by the company that administers the credit/debit card payments."[2]

C.   **FACTS RELATING TO NAMED REPRESENTATIVE PLAINTIFFS**

       Plaintiff Max Story.

46.   Plaintiff Max Story is a consumer protection attorney representing low-income consumers and his wife is a pediatric mental health therapist who worked for seven years on the campus of Fletcher High School. They have two children who attend Duval County Public Schools and have both served on the board of each of their children's parent teacher associations.

47.   In or around September 2015, Mr. Story created a MySchoolBucks account to pay for one of his children's school lunches and other fees. Based on the representations on Heartland's website, Mr. Story believed that the fees were established by, and went entirely to, the school district. Despite he and his wife being big supporters of and very involved in the public schools, they never were informed that the fees were in fact undisclosed Credit/Debit Card Surcharges imposed and collected entirely by Heartland.

48.   From September 2015 through May 2019, Mr. Story paid 56 "Program Fees" to Heartland.

---

[2] http://www.soudertonsd.org/parents-students/food-services/myschoolbucks-convenience-fee-increase. Site last visited December 4, 2019.

49.   When Mr. Story's deposit to his children's MySchoolBucks accounts was made from his checking account with a debit card, he was charged a "Program Fee" of $1.95 for each transaction regardless of the amount. In reality, this fee was a Debit Card Surcharge imposed by Heartland, but not properly disclosed.

50.   When Mr. Story's deposit to his child's MySchoolBucks account was made from his credit card, he was charged a flat fee or "Program Fee" of $2.49 for each transaction, regardless of the amount. In reality, this amount was a Credit Card Surcharge imposed by Heartland but not properly disclosed.

51.   The vast majority of Mr. Story's deposits were for $45. The $2.49 Credit/Debit Card Surcharge represents 5.53% of the deposit being made to his child's MySchoolBucks account.

52.   Despite Heartland's representation that its program was "free," it was not free as a Program Fee was charged each and every time Mr. Story put funds into his MySchoolBucks account.

53.   Despite Heartland's representation that the School District "required" Mr. Story to pay a Program Fee, the Program Fee was actually charged and collected by Heartland.

54.   Despite Heartland's representation that the Program Fees paid by Mr. Story were being paid to the school district, Duval County School District actually did not retain any of the Program Fees paid by Mr. Story.

55.   Mr. Story paid Program Fees to Heartland believing them to have been required by and paid to the school district. He was unaware that the fees were actually Credit/Debit Card Surcharges or Convenience Fees charged for using his credit card and debit card to put money into the lunch accounts of his children. Had he known the true nature of the fees, he would not have paid them and would have contacted his bank and Credit Card Company to complain about the fees. He only paid the program fees because he was deceived by Heartland.

Plaintiff Nancy Murrey-Settle

56.   Plaintiff Nancy Murrey-Settle is an employee of the Duval County School District and was a foster parent to one child in 2012, who attended and still attends Duval County Public Schools. As part of the State of Florida's foster parent program, the child received free lunch. When Ms. Murrey-Settle's child was in the second grade and Ms. Murrey-Settle wanted to be in a position to provide a treat from the school's cafeteria upon occasion, such as a weekly ice cream, as a reward system to encourage the child's good behavior. As is the case in many school districts who implement the payment processing system, the school would not accept cash payments at the time. Ms. Murrey-Settle was therefore forced to create a MySchoolBucks account for her foster child thinking that she could place $10.00 into the account for the purpose of rewarding the little girl.

57.   Ms. Murrey-Settle was charged a $2.49 "Program Fee" on the $10 deposit into her MySchoolBucks account. In reality, the fee was a Credit Card Surcharge imposed by Heartland but not properly disclosed.

58.   The following year, Ms. Murrey-Settle adopted the foster child and she continues to attend public school in Duval County, Florida. Ms. Murrey-Settle routinely placed money into the MySchoolBucks account and was charged Credit Card Surcharge disguised as a "Program Fee" for each deposit over a period of approximately four years because it was imperative that her child have access to simple carbohydrates in order to manage a genetic condition.

59.   Despite Heartland's representation that its program was "free," it was not free as a Program Fee was charged each and every time Ms. Murrey-Settle put funds into her MySchoolBucks account.

60.   Despite Heartland's representation that the School District "required" Ms. Murrey-Settle to pay a Program Fee, Heartland required the fee.

61.   Despite Heartland's representation that the Program Fees paid by Ms. Murrey-Settle were being paid to the school district, Duval County School District actually did not retain any of the Program Fees paid by Ms. Murrey-Settle.

62.   Ms. Murrey-Settle paid Program Fees to Heartland believing them to have been required and paid to the school district. She was unaware that the fees were actually Credit/Debit Card Surcharges or Convenience Fees charged for using

her credit card and debit card to put money into the lunch accounts of her child. Had

she known the true nature of the fees, she would not have paid them and would have

contacted her bank and Credit Card Company to complain about the fees. She only

paid the program fees because she was deceived by Heartland.

63.   Once her child reached the sixth grade and was more capable of

handling cash responsibly, Ms. Murrey-Settle no longer made deposits into the

MySchoolBucks account in order to stop paying the excessively high fees. Ms.

Murrey-Settle believes that she made her last deposit into the MySchoolBucks

account sometime in 2016.

64.   Sometime after this lawsuit was originally filed, Heartland began

sending Ms. Murrey-Settle emails informing her that there was a balance remaining

in her MySchoolBucks account and urging her to sign in to her account. She went to

the website to log in and retrieve the funds in the account only to read the "pop-up"

notification that she would have to agree to the new Terms of Service in order to

access her account, including consent to binding mandatory arbitration of all past

and future claims, a class action ban and to specifically waive any right to participate

in the instant lawsuit originally filed by Mr. Story. She did not agree to the new

Terms and Conditions.

65.   Ms. Murrey-Settle was later unable to access her account and retrieve

the funds that Heartland said were in her account.

25

D.   CLASS ALLEGATIONS

66.   Pursuant to Federal Rule of Civil Procedure 23(a), (b) (2) and (b) (3),

Plaintiffs bring this action on behalf of themselves and all others similarly situated.

The Classes are defined as:

NATIONAL CLASS: All persons in the United States (except those persons who reside in the State of New Jersey) who entered into a MySchoolBucks Terms of Service Agreement with Heartland in a form substantially similar to Exhibit D, and who paid a MySchoolBucks Program Fee to Heartland.

FLORIDA SUBCLASS: All persons who reside in the State of Florida who entered into a MySchoolBucks Terms of Service Agreement with Heartland in a form substantially similar to Exhibit D, and who paid a MySchoolBucks Program Fee to Heartland.

Collectively the ("Class")

67.   Excluded from the Classes are: (a) Defendant, any entity in which

Defendant has a controlling interest, and its legal representatives, officers, directors,

employees, assigns, and successors; and (b) the judge to whom this case is assigned

and any member of the judge's immediate family.

68.   Heartland's Terms of Service Agreement dictates that New Jersey law

"governs these Terms of Use." The statute of limitations is six years for the New

Jersey Consumer Fraud Act ("NJCFA"), the New Jersey Truth-in-Consumer

Contract Warranty and Notice Act ("TCCWNA") and for Breach of Contract. The

Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") claim is subject to

a four-year statute of limitations.

69.   Plaintiffs can identify and ascertain all other class members from Heartland's business records. These records are computerized and will reflect which customers were charged and paid Heartland's deceptive and unfair "Program Fee" which was actually an undisclosed Credit/Debit Card Surcharge. Thus, Plaintiffs' proposed classes are ascertainable.

70.   **Numerosity:** Plaintiffs do not know the exact size of the classes because this information is in Heartland's exclusive control. However, based on the nature of the commerce involved and the size and scope of Heartland's business, Plaintiffs believe the class members number in the tens of thousands and that class members are dispersed throughout the United States, including Florida. Therefore, joinder of all class members would be impracticable.

71.   **Typicality:** Plaintiffs' claims are typical of other class members' claims because Plaintiffs and all class members were subject to a standard form Terms of Service Agreement and were charged the same unlawful MySchoolBucks Program Fee by Heartland, which was actually a Credit/Debit Card Surcharge.

72.   Before this Amended Complaint was filed, Plaintiffs – through counsel – made Freedom of Information Act requests to various school districts identified through public records as having a contractual arrangement with Heartland similar to Duval County Public Schools. Plaintiffs received documentation and reviewed Merchant Agreements between Heartland and a multitude of school districts in

California, Colorado, Florida, Illinois, Louisiana, New Jersey and New York. It appears from this review that Heartland used standard form Merchant Agreements during the class period that do not materially vary from one school district to another. While the amounts charged to the parents for Credit/Debit Card Surcharges may vary slightly by school, the differences are minor and merely mathematical. Regardless, Heartland uniformly fails to accurately disclose the Credit/Debit Card Surcharges and systematically states that only a Program Fee or Membership Fee may be required by the school. Each of Heartland's Merchant Agreements dictate that the rules imposed by Visa, Mastercard, Discover and American Express must be followed, including any fees charged as Credit/Debit Card Surcharges.

73. **Commonality and Predominance:** Questions of law and fact common to the Class and Subclass exist and predominate over questions affecting only individual members, including, *inter alia*, the following:

> a. Whether Heartland's representations regarding the MySchoolBucks Program Fee are unfair and deceptive because the fees are actually Credit/Debit Card Surcharges;
>
> b. Whether Heartland's Term of Service Agreement section titled "Program Fee or Membership Fee" deceptively explains its Credit/Debit Card Surcharge in violation of the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-1 *et seq.*;

c.   Whether Heartland violated the Rules imposed by Visa, Mastercard, Discover, American Express or ACH for imposing surcharges for use of a credit or debit card;

d.   Whether the aforementioned violations of the NJCFA and Heartland's failure to comply with the disclosure requirements imposed by Visa, Mastercard, Discover, American Express, or ACH for imposing Credit/Debit Card Surcharges constitutes violations of the New Jersey Truth-in-Consumer Contract Warranty and Notice Act, N.J.S.A. § 56:12-14 *et seq.*, specifically N.J.S.A. §56:12-15;

e.   Whether Heartland violated FDUTPA by charging a Credit/Debit Card Surcharge and/or by failing to disclose that the Program Fee was actually a Credit/Debit Card Surcharge;

f.   Whether the contracts between Heartland and the parents (including Plaintiffs) was breached;

g.   Whether Heartland's actions have proximately caused an ascertainable loss to Plaintiffs and members of the Class and Subclass and, if so, the proper measure of damages; and

h.   Whether Plaintiffs and Class members are entitled to declaratory and injunctive relief.

74.   **Adequacy:** The named Plaintiffs will fairly and adequately represent and protect the interest of the members of the Class because they possess no interest antagonistic to the class members they seek to represent, and because the adjudication of their claims will necessarily decide the identical issues for all other class members. Whether the NJCF, TCCWNA, and FDUTPA were violated and whether Heartland breached its contract with parents involve predominating common issues that will be decided for all consumers who entered into similar or identical Terms of Service Agreements. There is nothing peculiar about the Plaintiffs' situations that would make them inadequate class representatives.

75.   Plaintiffs have retained counsel competent and experienced in both consumer protection and class action litigation.

76.   **Superiority:** A class action is superior to other methods for the fair and efficient adjudication of this controversy because the damages suffered by each individual Class member are relatively modest, compared to the expense and burden of individual litigation. It would be impracticable for each Class member to seek redress individually for the wrongful conduct alleged herein. It would be difficult, if not impossible, to obtain counsel to represent Plaintiffs on an individual basis for such small claims. More importantly, the vast majority of Class members are not aware that Heartland's MySchoolBucks Program Fee violates the NJCFA, FDUTPA and/or the TCCWNA and if Heartland breached its contract with parents. Practically

speaking, a class action is the only viable means of adjudicating the individual rights of Plaintiffs and the Classes. There will be no difficulty in the management of this litigation as a class action as the legal issues affect a standardized pattern of conduct by Defendant and class actions are commonly used in such circumstances. Furthermore, since joinder of all members is impracticable, a class action will allow for an orderly and expeditious administration of the claims of the Class and Subclass and will foster economies of time, effort and expense.

COUNT I:
Violation of the New Jersey Consumer Fraud Act
N.J.S.A. §56:8-2.1 *et seq.*
On Behalf of the Class

77.   Plaintiffs, on behalf of themselves and all others similarly situated, repeat and reallege paragraphs 1 through 76 as if expressly set forth in this Count.

78.   N.J.S.A. §56:8-2. declares that:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice; …

79.   Plaintiffs are both "persons" and "consumers" pursuant to N.J.S.A. §56:8-1(d), as they and all Class members are natural persons as defined therein.

80.   Defendant is a "person" pursuant to N.J.S.A. §56:8-1(d), as it is a business entity, corporation or company as defined therein.

81.   Defendant's MySchoolBucks service is "merchandise" pursuant to N.J.S.A. §56:8-1(c), as it is a service offered directly or indirectly to the public for sale as defined therein.

82.   Defendant engages in the sale of merchandise pursuant to N.J.S.A. §56:8-1(e), as it offers its MySchoolBucks service directly or indirectly to the public for sale.

83.   Heartland engaged in an unconscionable, unfair, deceptive, fraudulent and/or misleading pattern and practice by making misleading or false statements regarding fees charged to Plaintiffs and the putative Class members, fraudulently omitting required disclosures and charging Surcharges in excess of those permitted by applicable rules and the Merchant Agreements between Heartland and school districts of which parents are intended third-party beneficiaries. More specifically, those violations were:

a.   Heartland enters into uniform Merchant Agreements with various schools throughout the United States. In those Merchant Agreements, Heartland regularly imposes a Credit and/or Debit Card Surcharge to be paid by either the School or parents. Heartland subsequently enters into standard form MySchoolBucks Terms of Service Agreements with

parents where it misrepresents the surcharge as a "program fee" required by the school districts:

Program Fee or Membership Fee

Your school district may require a program fee or membership fee for your use of the Service. If you are required to pay a program fee, you will be notified on a screen prior to completing the payment transaction and any such program fee will be required for each payment you make using the Service.

Exhibit D, Terms of Service (emphasis added). This language is unfair and deceptive because the Merchant Agreement with the school districts reveals that the true nature of the charge is a Credit/Debit Surcharge and not a program fee imposed or collected by the school.

    b.   Under the "Payments to Schools" section of the Terms of Service Agreement, Heartland states "Your child's school receives the full payment." This statement is untrue because the money charged as Program Fees are not given to schools.

    c.   Additionally, Heartland's MySchoolBucks website states that MySchoolBucks is "free" and that the school districts impose the Fee:

        Is there a fee for using MySchoolBucks?

Signing up for MySchoolBucks is **free**. Depending on your school/district and order/item you are purchasing, you may be required to pay a program or membership fee.[3]

(Emphasis added).

This statement is false or deceptive because it is not free and Heartland knew that parents would be required to pay Credit/Debit Card Surcharges every time money is placed in the child's account.

d.   Heartland made omissions of material facts by failing to disclose the true nature of the program fees as Credit/Debit Card Surcharges, the basis for the imposition of the program fees, where the money went, and how the amount of the fee was determined. Specifically, because the fees are actually a Credit/Debit Card Surcharge resulting from its Merchant Agreement, it should have explained these facts to parents in accordance with the disclosure requirements imposed by the Credit Card Companies.

e.   Heartland made further omissions when it failed to comply with the Credit Card Company disclosure requirements for Credit/Debit Card surcharges that are clearly intended to benefit the consumer. Namely, Merchants must clearly and prominently disclose to consumers any

---

[3] https://www.myschoolbucks.com/ver2/help/gethelp Site last visited December 4, 2019.

surcharge that will be assessed, including (i) the exact amount or percentage; (ii) a statement that the surcharge is assessed by the merchant and is applicable only to credit card transactions; and (iii) a statement that the surcharge amount is no greater than the amount paid by the merchant to its payment processor for processing the transaction.

f.   Heartland's Program Fees as imposed on Plaintiffs and the putative Class members were unfair in that their actual status as Credit/Debit Card Surcharges was never disclosed to the consumer and because the amount of the charge exceeded the rules of the Credit Card Companies because surcharges must be no more than the cost of credit and have a cap far below the amounts set by Heartland.

84.   The scheme perpetrated by Heartland in the way it assessed its Program Fees was deceptive and unfair, and its explanation for the program fees it charged was false and/or misleading because Heartland failed to disclose that the fees are actually Credit/Debit Card Surcharges. Defendant's conduct lacks honesty in fact, fair dealing and good faith and has the capacity to mislead consumers acting reasonably.

85.   Further, Heartland's omission of required disclosures was unlawful and injurious to Plaintiffs. Full and fair disclosure of the nature of the fees, the cost of the fees and who was charging and receiving the fees are all necessary information

for a consumer in deciding whether to accept and pay the Credit/Debit Card Surcharge. Consumers like Plaintiffs did not understand the extent to which they could reject or challenge the Surcharge, did not have a practicable option to comparison shop under the circumstances, and also were unaware of who or how to protest or question the legitimacy or the amount of the Surcharge. Had Plaintiffs known the true nature of the Program Fees as Credit/Debit Card Surcharges, they would not have paid the fee and/or would have challenged the fee with their credit card companies.

86.   Such practices contravene the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-1, *et seq*.

87.   N.J.S.A. § 56:8-2.11 provides that "Any person violating the provisions of the CFA shall be liable for a refund of all monies acquired by means of any practice declared herein to be unlawful."

88.   As a result of Defendant's aforementioned violations, Plaintiff Story suffered an ascertainable loss of an amount no less than 56 payments of the $1.95 debit card fee or the $2.49 credit card fee.

89.   As a result of Defendant's aforementioned violations, Plaintiff Murrey-Settle suffered an ascertainable loss of an amount no less than paying the $2.49 credit card fee over the course of around four years on each of her approximately $10 deposits.

90.   As a result of Defendant's aforementioned violations, Plaintiffs and putative Class members are due to receive their actual damages equal to the ascertainable loss of all program fees paid to Heartland during the class period.

91.   Alternatively, Plaintiffs and Class members suffered an ascertainable loss in that Heartland caused them to pay money in excess of the allowable Credit/Debit Card Surcharges allowed under the Rules of the Credit Card Companies. The Credit Card Companies all limit Surcharges to the merchant's cost of credit. Because Heartland charges far in excess of the cost of accepting Credit/Debit Card payments, it violates these limits to the detriment of Plaintiffs and the putative class.

92.   This misrepresentation of the Credit/Debit Card Surcharge as a "Program Fee" required by and paid to the school had a direct bearing on Plaintiffs' decision to pay the fees. Had Plaintiffs been provided with actual disclosure of the Credit/Debit Surcharges, they would have challenged the assessment of and amounts of the fee and would not have paid the "Program Fee."

93.   As a direct and proximate result of Heartland's violations of the N.J.S.A. § 56:8-2, as set forth in the preceding paragraphs, Plaintiffs suffered a concrete and ascertainable loss in the amounts of each $2.49 and $1.95 Surcharge imposed upon them by Heartland each time the placed funds into their children's MySchoolBucks account, as set forth above.

94.   But for Heartland's unconscionable acts and misrepresentations in violation of the CFA, Plaintiffs would not have suffered any damage. Said another way, Plaintiffs' damages are the direct and proximate result of Defendant's violations of the CFA, in that their loss flowed directly from Heartland's acts.

95.   Plaintiffs and Class members are entitled to treble damages pursuant to N.J.S.A. § 56:8-19.

96.   In accordance with N.J.S.A. § 56.8-19 and N.J.S.A. § 56.12-17, Plaintiffs and Class members are entitled to attorney's fees and litigation costs.

<u>**COUNT II:**</u>
Violation of the New Jersey Truth-in-Consumer Contract, Warranty and Notice Act, ("TCCWNA") N.J.S.A. § 56:12-14 *et seq.*
On Behalf of the Class

97.   Plaintiffs, on behalf of themselves and all others similarly situated, repeat and reallege paragraphs 1 through 76 as if expressly set forth in this Count.

98.   The New Jersey Truth in Consumer Contract, Warranty and Notice Act (TCCWNA) § 56:12-14 *et seq.,* prohibits sellers from "offer[ing] to any consumer or prospective consumer or enter[ing] into any written consumer contract or giv[ing] or display[ing] any written consumer warranty, notice or sign . . . which includes any provision that violates any clearly established legal right of a consumer or responsibility of a seller . . . as established by State or Federal Law . . . ." N.J.S.A. § 56:12-15.

99.   Plaintiffs and all members of the Class are "consumers" within the meaning of TCCWNA.

100.   Heartland is a "seller" within the meaning of TCCWNA.

101.   Heartland's MySchoolBucks Terms of Service Agreement is a written agreement between Heartland and Plaintiffs which is both a "consumer contract" and a notice within the meaning of TCCWNA.

102.   Heartland gave, displayed, offered and/or entered into the MySchoolBucks Terms of Service Agreement with Plaintiffs as well as with all members of the Class.

103.   Heartland's contract with parents contains a provision that violates clearly established legal rights of consumers by mischaracterizing the Credit/Debit Card Surcharges as "Program Fees" in its Terms of Service because the Merchant Agreements with schools clearly require compliance with rules promulgated by the Credit Card Companies providing for registration, disclosures and limitations on the amount charged.

104.   Namely, Merchants accepting credit card payments must clearly and prominently disclose to consumers any Credit/Debit Card Surcharge that will be assessed, including (i) the exact amount or percentage; (ii) a statement that the surcharge is assessed by the merchant and is applicable only to credit card transactions; and (iii) a statement that the surcharge amount is no greater than the

amount paid by the merchant to its payment processor for processing the transaction. *See, e.g.,* 5.6.1.6 VISA Rules, US Credit Card Surcharge Maximum Amount – US Region and US Territories; 5.6.1.7 VISA Rules, US Credit Card Surcharge Disclosure Requirements – US Region and US Territories; 5.6.2.1 VISA Rules, Convenience Fees – AP, CEMEA, and US Regions.; Mastercard Rule 5.11.2.3 Charges to Cardholders, Requirements for Merchant Disclosure of a Surcharge at the POI.

105.   Both Visa and Mastercard prohibit ANY Surcharge to be imposed on debit cards. *Id*.

106.   Heartland's charges to Plaintiffs and the putative Class members further violates the TCCWNA because the Credit/Debit Card Surcharges exceeded the rules of the card network associations. Specifically, all Surcharges must be clearly disclosed and explained. Second, the amount of the surcharge is limited to the cost of credit but can never exceed 4%. In the case of Plaintiffs, the credit card surcharges exceeded both the cost of credit and the applicable cap. *See, e.g.,* 5.6.1.6 VISA Rules, US Credit Card Surcharge Maximum Amount – US Region and US Territories; 5.6.1.7 VISA Rules, US Credit Card Surcharge Disclosure Requirements – US Region and US Territories; 5.6.2.1 VISA Rules, Convenience Fees – AP, CEMEA, and US Regions.

107.   Plaintiffs have a clearly established right to receive a clear and accurate disclosure of both the nature and the amount of any surcharge imposed because credit and/or debit cards were used by Heartland to make these payments. Specifically, Plaintiffs have a clearly established right to receive an accurate disclosure of the exact amount or percentage charged, a statement that the surcharge is assessed by the merchant and is applicable only to credit card transactions, and a statement that the surcharge amount is no greater than the amount paid by the merchant to its payment processor for processing the transaction.

108.   The inaccurate and misleading Program Fee disclosure provisions in Heartland's Terms of Service constitute a violation of TCCWNA in that they deprive Plaintiffs of the clearly established right to receive a clear and accurate disclosure of the true nature and amount of any surcharge imposed.

109.   In addition, Heartland's inclusion of the inaccurate and misleading Program Fee disclosure provisions in the Terms of Service constitute a violation of TCCWNA in that Heartland has a clearly established responsibility to provide clear and accurate disclosure of the true nature and amount of any surcharge imposed.

110.   Plaintiffs, and all members of the Class, suffered harm as a result of the inclusion of prohibited language by Heartland in the Terms of Service, and therefore they are "aggrieved consumers" within the meaning of N.J.S.A. § 56:12-17.

111.   Specifically, Plaintiff Story is an aggrieved consumer because he incurred monetary damages in loss of an amount no less than 56 payments of the $1.95 debit card fee and $2.49 credit card fee, as a consequence of Heartland's inclusion of prohibited provisions in the Terms of Service and other writings offered to and entered into by Plaintiffs.

112.   Specifically, Plaintiff Murrey-Settle is an aggrieved consumer because she incurred monetary damages in an amount of no less than paying the $2.49 credit card fee over the course of around four years on each of her $10 deposits, as a consequence of Heartland's inclusion of prohibited provisions in the Terms of Service and other writings offered to and entered into by Plaintiffs.

113.   Alternatively, Plaintiffs are aggrieved consumers in that the misleading and violative language of Heartland's surcharge disclosures deterred Plaintiffs from seeking other less expensive methods to pay for school fees. Specifically, had they not been deterred by Heartland's inclusion of language stating that "your school district may require a program fee or membership fee for your use of the [MySchoolBucks payment service]" and "your child's school receives the full payment," Plaintiffs would have sought and utilized alternate methods to pay for school fees.

114.   As a result of Heartland's violations of TCCWNA as alleged herein, Plaintiffs and putative Class members are entitled to damages pursuant to N.J.S.A. §

56:12-17 which include actual damages and statutory damages of not less than $100 per violation, together with reasonable attorney fees and costs.

<div align="center">

COUNT III:
Breach of Contract
On Behalf of the Class

</div>

115.   Plaintiffs, on behalf of themselves and all others similarly situated, repeat and reallege paragraphs 1 through 76 as if expressly set forth in this Count.

116.   Plaintiffs assert this Breach of Contract Claim in the alternative to the Consumer Protection Statutory violations asserted in Counts I, II, and III.

117.   Plaintiffs and Class members contracted with Heartland for the use of the MySchoolBucks program. **Exhibit D**, Terms of Service (May 3, 2016 version).

118.   Plaintiffs and Class members gave consideration and performed all conditions precedent to filing this action.

119.   The Paragraph titled "Program Fee or Membership Fee" of the standardized MySchoolBucks program Terms of Service contract between Plaintiffs and Class members stated that a school district may require a program fee and that the school would receive "the full payment:"

> Your school district may require a program fee or membership fee for your use of the Service. If you are required to pay a program fee, you will be notified on a screen prior to completing the payment transaction and any such program fee will be required for each payment you make using the Service.

The Agreement further stated:

Payments to Schools

You may make payments to your child's school account using a credit card. Your credit card provider may have imposed a maximum amount which can be placed on your credit card. **Your child's school receives the full payment.** Payments are processed promptly for your child's use. …

(Emphasis added).

120.   Because Heartland contracted to send the "full payment" to the school including the MySchoolBucks Program Fee, it breached its contract by not paying the Program Fee to the school as promised. Heartland has materially breached the MySchoolBucks Terms of Service with Plaintiffs and putative Class members.

121.   As a direct and proximate result of Heartland's material breach, Plaintiffs and putative Class members are entitled to a refund of the amount paid as "Program Fees."

122.   Plaintiff and Class members suffered actual damages in the amount of Program Fees paid as a direct and proximate result of Defendant's breach.

<div align="center">

COUNT IV:
Violation of the Florida Deceptive and Unfair Trade Practices Act (FDUTPA)
On Behalf of the Florida Subclass Only

</div>

123.   Plaintiffs, on behalf of themselves and all others similarly situated, repeat and reallege paragraphs 1 through 76 as if expressly set forth in this Count.

124.   Heartland's Terms of Service Agreement dictates that New Jersey law "governs these Terms of Use." Therefore, to the extent that claims arise outside the

<div align="center">44</div>

Terms of Use Agreement, they are not governed by New Jersey Law. This Count arises outside the Terms of Use Agreement.

125. Florida law declares that "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." Fl. Stat. § 501.204(1).

126. Chapter 501 of the Florida Statutes governs Consumer Protection generally. Fla. Stat. § 501.0117, prohibits sellers of goods and services from imposing a surcharge on Florida buyers for using a credit card. Specifically, Fla. Stat. § 501.0117(1) states:

> A seller or lessor in a sales or lease transaction may not impose a surcharge on the buyer or lessee for electing to use a credit card in lieu of payment by cash, check, or similar means, if the seller or lessor accepts payment by credit card. A surcharge is any additional amount imposed at the time of a sale or lease transaction by the seller or lessor that increases the charge to the buyer or lessee for the privilege of using a credit card to make payment.

127. Persons imposing surcharges in violation of this provision are guilty of a second-degree misdemeanor. Fla. Stat. § 501.0117(2).

128. Heartland engaged in unfair, unconscionable or deceptive acts and practices by charging Plaintiffs and members of the Florida Subclass Credit/Debit Card Surcharges in violation of Fla. Stat. § 501.0117.

129.   Heartland also engaged in unfair, unconscionable or deceptive acts and practices by deceptively labeling its Credit/Debit Card Surcharge as a "Program Fee" so as to avoid the protections provided to Florida consumers by Fla. Stat. § 501.0117. By labeling the Surcharge as a "Program Fee," Florida consumers like Plaintiffs and members of the Florida Subclass were unable to determine that the fee was actually related to their credit card payments and therefore prohibited in Florida as a Surcharge.

130.   Plaintiffs Story and Murrey-Settle would not have paid the Credit/Debit Card Surcharges imposed by Heartland if they had been properly labeled as Surcharges.

131.   Because Credit/Debit Card surcharges are prohibited by Fla. Stat. § 501.0117, and Heartland deceptively labeled its Surcharges as Program Fees, Plaintiffs and members of the Florida Subclass have suffered actual damages in the amount of all "Program Fees" paid during the class period.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that the Court enter an Order:

A.   Certifying this action as a class action as provided by Rule 23(a) and (b) of the Federal Rules of Civil Procedure, appointing Plaintiffs as class representatives, and appointing the undersigned to act as Class Counsel;

B.   Declare that Heartland is financially responsible for notifying all Class members;

C.   For injunctive relief prohibiting Heartland from future violations of the Consumer Fraud Act, N.J.S.A. § 56:8-1 *et seq.*, Truth-in-Consumer Contract, Warranty and Notice Act, N.J.S.A. § 56:12-14 *et seq.*, and FDUTPA, and requiring Heartland to comply with these statutes and all applicable rules and regulations;

D.   Awarding disgorgement of all the MySchoolBucks Program Fees Heartland collected and retained from Plaintiffs and Class members;

E.   Awarding actual damages, punitive damages, treble damages pursuant to N.J.S.A.§ 56:8-19, and actual and statutory damages pursuant to N.J.S.A. § 56: 12-17;

F.   Awarding reasonable attorneys' fees and costs of suit in connection with this action pursuant to N.J.S.A. § 56:8-19, N.J.S.A. § 56:12-17; and Fla. Stat. §501.2105;

G.   Declaring that Heartland is in breach of its contracts with Plaintiffs and Class members and awarding compensatory damages;

H.   Awarding pre-judgment and post-judgment interest; and

I.   For such other and further relief as Plaintiffs and Class members may be entitled or as the Court deems equitable and just.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Respectfully submitted this 5th day of February, 2021.

VARNELL & WARWICK, P.A.

s/ Brian W. Warwick

Brian W. Warwick, FBN: 0605573

Janet R. Varnell, FBN: 0071072

Matthew T. Peterson, FBN: 1020720

Erika Willis, FBN: 100021

1101 E. Cumberland Ave., Suite 201H, #105

Tampa, Florida 33602

Telephone: (352) 753-8600

Facsimile: (352) 504-3301

bwarwick@varnellandwarwick.com

jvarnell@varnellandwarwick.com

mpeterson@varnellandwarwick.com

ewillis@varnellandwarwick.com

awallace@varnellandwarwick.com

kstroly@varnellandwarwick.com

Stephanie Glaberson (Admitted *Pro Hac Vice*)

PUBLIC JUSTICE, P.C.

1620 L Street NW, Suite 630

Washington, DC 20036

Telephone: (202) 797-8600

sglaberson@publicjustice.net

Attorneys for Plaintiffs

48

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 5th day of February, 2021, I electronically

filed the foregoing with the Clerk of the Court using the CM/ECF system, which

will send a notice of electronic filing to all counsel of record.

/s/ Brian W. Warwick
BRIAN W. WARWICK

EXHIBIT A

DocuSign Envelope ID: 51B280EF-9150-486F-8968-32B22F62438A

Heartland

K-12 MERCHANT PROCESSING AGREEMENT
☐ Card Only   ☐ ACH Only   ☒ Dual

HEARTLAND CONTACT INFORMATION

RM: Jeff Olek	**Phone:** 800-423-2113	**Fax:** 585-227-8594
Affiliate/Partner ID : K12	**Affiliate Name:** MySchoolBucks	**Current MID:** 650000007885703

COMPANY INFORMATION

Merchant DBA Name: Duval County Public Schools   **DBA Phone#:** 904-732-5117
Address: 2924 Knights Lane East, Bldg 6   **# Locations:** N/A
City: Jacksonville   **State:** FL   **Zip:** 32216
CS Phone #: 800-803-6755   **Fax #:** 585-227-8594
Primary Contact Name: Dr. Patricia S. Willis   **Phone #:** 904.390.2115
Authorized to Purchase: ☒ Yes ☐ No
Secondary Contact Name: **Phone #:**
Authorized to Purchase: ☒ Yes ☐ No
Email Address: HSSActivations@e-hps.com
        (Heartland InfoCentral Admin User Email Address)
Email Contact: First Name: **Last Name:**
Website Address: https://dcps.duvalschools.org/
District Name: Duval County Public Schools   **Federal Tax ID / EIN:** 596000589
        (Please Complete – Must correspond with IRS Filing Name)   (Must correspond with Legal Name)
Address: Same as above   **Phone #:** Same as above
City: Same as above   **State:** Same as above   **Zip:** Same as above

CARD FEE SCHEDULE

Service Requested	Discount Rate	Discount Per Item	Trans Fee Dial	Trans Fee IP			
Visa	%	$ 2.49			**Annual Volume:** $ 25,000	**Average Ticket:** $ 45.00
MasterCard	%	$ 2.49	$ 0	$ 0		**High Ticket:** $ 45.00
Discover/JCB	%	$ 2.49			☒ Service Fee (Pass Through/Single Transaction)	
TSYS Authorization	%	$	$	$	☐ COST PLUS	
PIN Debit*					*Plus Applicable Debit Network Fees	

Fee Model: ☐ District Absorbed   ☒ Parent Paid

RECURRING FEES

				SETTLEMENT
Chargeback Fee:	$0	Voice Authorization Fee:	$0	☐ Monthly ☒ Daily Net

INTERCHANGE QUALIFICATION

INTERCHANGE QUALIFICATION	CARD ACCEPTANCE	DEPOSIT METHOD
☒ MOTO / Internet ☐ Retail ☐ Small Ticket	☒ All Cards Accepted	☒ Standard

ACH FEE SCHEDULE

Transaction Fee	$ 1.95	%	**Annual ACH Volume:** $ 2,500.00	**Average ACH Amount:** $ 21.00
Monthly Fee		$ 0	**Average # of ACH Transactions per Month:** 40	
Return Item Fee		$ 0	**Max ACH Limit:** 500.00	

Re-presentment: ☐ Yes ☒ No   (Limitation of 2 per NACHA guidelines)   **Re-presentment Fee: $N/A**
☐ K12-OnePay Program
  Fee: Single: $12.95   Multi: $26.95   ACH Settlement Method: ☒ Daily Net ☐ Monthly Net

DocuSign Envelope ID: 51B280EF-9150-486F-8968-32B22F62438A

MERCHANT DETAIL

Type of Business: [X] Public [ ] Private	Date Business Started: 01/01/1900	**Business is Conducted: 100% Consumer**
Type of Ownership: [X] Corporation [ ] L.L.C.		Do you process web based sales through HPS: Yes

What Products and / or services do you provide: Payment for nutrition and school fees

Is there a peak week / date in the month for processing recurring transactions: (i.e., 1st and 15th):	N/A

Define your Refund Policy: Managed by Heartland School Solutions

Sales Method					Card Processing Method	
On Premise Face to Face Sales	0 %	Mail Order Sales	%	Card Swipe		0 %
Off Premise Face to Face Sales	%	Real-Time Internet	%	Keyed / Card Not Present		100 %
Inbound Telephone Order Sales	%	Internet (keyed)	100 %	**Total = 100%**		
Outbound Telephone Order Sales	%	Recurring Billing	%	**ACH Processing Method**		
		Total = 100%		PPD	%	WEB 100 %
What percentage of your Bankcard volume is future delivery			%	CCD	%	TEL %

PCI Compliance

Is your business PCI Compliant: [X] Yes [ ] No

Does your company utilize a Data Storage Entity or Merchant Servicer that has access to card member data (i.e., Payment gateway or data warehouse, etc.): [ ] Yes [X] No

If yes, provide the name of the Data Storage Entity or Merchant Servicer being utilized: N/A

PCI DSS and Card Network rules prohibit storage of sensitive authentication data after the transaction has been authorized (even if encrypted). If you or your POS system store, process, or transmit full cardholder's data, then you (merchant) must validate PCI DSS compliance. If you (merchant) utilize a payment application the POS software must be PA DSS (Payment Application Data Security Standards) validated where applicable. If you use a payment gateway, they must be PCI DSS Compliant.

As required under the Payment Card Industry Data Security Standard (PCI DSS), I do hereby declare and confirm the following:

Merchant will maintain full PCI DSS compliance at all times and will notify Heartland when it changes its point of sale software, system, application or vendor: [ ] Yes [ ] No [X] N/A

Do your transactions process through any other Third Parties (i.e. web hosting companies, gateways, corporate office): [ ] Yes [ ] No [X] N/A

Merchant utilizes the services of a PCI SSC Qualified Integrator Reseller (QIR) when POS payment applications are utilized: [ ] Yes [ ] No [X] N/A

The signing merchant listed below has experienced an account data compromise.*: [ ] Yes [ ] No [X] N/A [ ] I have never accepted payment cards.)

If yes, what was the date of the compromise: N/A   (Copy of the completed forensic investigation is required with the app.)

The signing merchant listed below is storing Sensitive Authentication Data** (even if encrypted) after the transaction has been authorized: [ ] Yes [ ] No [X] N/A [ ] I have never accepted payment cards.)

Merchant utilizes an EMV enabled terminal: [ ] Yes [ ] No [X] N/A

*An Account Data Compromise is any incident that results in unauthorized access to payment card data and/or Sensitive Authentication Data.
**Sensitive Authentication Data is security related information (Card Verification Values, complete Magnetic Stripe Data, PINs, and PIN blocks) that is used to authenticate cardholders.

Please note that if you have indicated that your organization has experienced an account data compromise in the past, a PCI DSS Level 1 Compliance Assessment may be required upon Heartlands request. A compromise of cardholder data from your location(s) may result in the issuance of fines and/or penalties by the card brand, for which you will be responsible under your Merchant Agreement, notwithstanding this Compliance Statement.

It is imperative that you notify Heartland immediately should the information on this Compliance Statement change.

DocuSign Envelope ID: 51B280EF-9150-486F-8968-32B22F62438A

STATEMENT OPTIONS			DISPUTE LETTERS		
Statement Type:	☒ Standard		Mail Options:	☐ Legal ☐ DBA	
Mail Statements To:	☐ Suppress Stmts ☐ District		Electronic Options* ☒ Email ☐ Fax (*Select mail option as backup)		
☒ All Electronic Communications (Including ACH Returns):					
☐ Same Email as InfoCentral ☐ Preferred Email Address:					

AUTHORIZED SIGNER(S) INFORMATION

Is any owner, officer, director, employee, or agent a current or former senior official in the executive, legislative, administrative, military, or judicial branch of any government (elected or not); a senior official of a major political party; an executive of a government-owned commercial enterprise; a family member of any of the foregoing officials; or a close personal or professional associate of any of the foregoing officials? ☐ Yes ☒ No If "yes," please attach details.

(1) District/Authorized Signer Name: Dr. Patricia S. Willis			Title: Superintendent		
SSN: N/A			Driver's License #: N/A		
Home Address N/A		City: N/A	ST: NA	Zip: N/A	
(2) District/Authorized Signer Name:			Title:		
SSN: N/A			Driver's License #: N/A		
Home Address: N/A		City: N/A	ST: NA	Zip: N/A	

DEBIT / CREDIT AUTHORIZATION

Merchant certifies that any starter check or verification of business provided is for a business account in good standing and that the Business name on the below checking account is the same as the Business name on the enclosed Heartland Payment Systems Merchant Application. In addition, Merchant hereby authorizes Acquirer to debit and credit Merchant's checking/savings account. This authority shall remain in full force until (a) Acquirer has received written notification from Merchant of its termination; and (b) all obligations of Merchant to Acquirer under this Agreement have been paid in full.

Depository Bank Name: Bank of America Merrill Lynch		Phone #: 888-715-1000	
City: Jacksonville		ST: FL	Zip:

CARD	TRANSIT ROUTER / ABA NUMBER (9 digits)		ACCOUNT NUMBER (14 digits)
ACCOUNT TYPE (check one)	X Checking Savings GL		
FUNDS TRANSFER METHOD	X Deposits Fees Both	Name as it appears on Account:	

	TRANSIT ROUTER / ABA NUMBER (9 digits)		ACCOUNT NUMBER (14 digits)
ACCOUNT TYPE (check one)	X Checking ☐ Savings ☐ GL		
FUNDS TRANSFER METHOD	☐ Deposits x Fees ☐ Both	Name as it appears on Account:	

ACH	TRANSIT ROUTER / ABA NUMBER (9 digits)		ACCOUNT NUMBER (14 digits)
ACCOUNT TYPE (check one)	X Checking Savings GL		
FUNDS TRANSFER METHOD	Deposits X Fees Both	Name as it appears on Account:	

	TRANSIT ROUTER / ABA NUMBER (9 digits)		ACCOUNT NUMBER (14 digits)
ACCOUNT TYPE (check one)	☐ Checking ☐ Savings ☐ GL		
FUNDS TRANSFER METHOD	☐ Deposits ☐ Fees ☐ Both	Name as it appears on Account:	

AGREEMENT ACCEPTANCE, CERTIFICATION and CONSUMER REPORT AUTHORIZATION

Has your District filed Bankruptcy, had Judgments or Liens within the last 3 years: ☐ Yes ☒ No

Merchant authorizes Acquirer, reporting agency employed by Acquirer, or any agents thereof, to investigate the references, statements or data provided by Merchant or the undersigned for purposes of all matters generally connected to this business relationship. I further certify that I have received, read, understand and agree to the Merchant Processing Agreement Terms and Conditions which together with this application shall constitute the agreement(s) between the parties. **I further certify that this business or any Owner/Officer/Authorized Signer has never been terminated by any of the Card Brands** See attached signature page

X

(1) Authorized Signer Signature	Print Name & Title	Date
X		
(2) Authorized Signer Signature	Print Name & Title	Date

THE TERM OF THIS AGREEMENT IS 60 **MONTHS**

EXHIBIT B

GOVERNMENT AND PUBLIC EDUCATION CREDIT/DEBIT CARD PROCESSING AGREEMENT

TERMS & CONDITIONS

1. Services

HPS will, during the term of this Agreement and pursuant to its terms and conditions, (a) be responsible for and will settle funds with the Merchant; (b) provide the following payment processing solutions to the Merchant: (i) Web Payment Solutions; (ii) Cashiering Payment Solutions as may be selected by Merchant on the Merchant Application.

2. Definitions

2.1   **"Account"** means a commercial checking account maintained by Merchant for the crediting of collected funds and the debiting of fees and charges pursuant to the terms of this Agreement.

2.2   **"ACH"** means the Automated Clearing House service offered by the Federal Reserve.

2.3   **"Agreement"** means this Merchant Processing Agreement, the Merchant Application and the Addendum, as applicable. This contract incorporates the Merchant Processing Agreement, the Merchant Application, and the Addendum, as applicable, by reference, with the same force and effect as if it were given in full text. Upon request, HPS will make their full text available.

2.4   **"Authorization"** means the act of obtaining approval from the Card Issuer for an individual Transaction.

2.5   **"Card"** means a valid credit, debit, charge or other payment card accepted by Merchant under this Agreement with HPS.

2.6   **"Card Schemes" used interchangeably with Card Brands** means Visa U.S.A., Inc., Visa International, Inc., MasterCard International, Inc., Discover Financial Services or any other Card Issuer that provides Cards that are accepted by Merchant under this Agreement with HPS, including on-line debit card Transactions and on-line debit networks.

2.7   **"Card Issuer"** means the financial institution or company that has provided a Card to the Cardholder.

2.8   **"Cardholder" used interchangeably with Card Member** means the person or Card Member whose name is embossed upon the face of the Card.

2.9   **"Card-Not-Present Transaction"** means any Transaction for which required data is not electronically captured by reading information encoded in or on the Card and includes mail order, telephone order and Internet Transactions.

2.10   **"Cashiering Payment Solution"** means an automated solution which will allow Cardholders to pay Merchant via an HPS-provided virtual terminal or physical terminal.

2.11   **"Chargeback"** means the procedure by which (i) a sales Transaction (or disputed portion thereof) is returned to HPS by a Card Issuer because such item does not comply with the Card Issuer's applicable rules or operating regulations or for any other reason as provided in this Agreement and (ii) the Merchant's Account is debited for such return.

2.12   **"Convenience Fee"** means a fee charged to a consumer that will cover the costs of providing the convenient alternative payment solutions such as the Web Payment Solution and certain Cashiering Solutions.

2.13   **"Credit Voucher"** means a document or transaction executed by Merchant evidencing any refund or price adjustment relating to products or services to be credited to a Cardholder account.

2.14   **"Debit Networks"** means the authorization networks utilized by Merchant for PIN Debit Transactions.

2.15   **"EMV Card"** refers to a form of smart payment card with technical standards originally created by Europay, MasterCard and Visa (EMV) embedded with a chip containing encrypted Cardholder account information, which is readable by an EMV-enabled device. An EMV Card may be used by: (1) inserting it into a card reader that is integrated with a point of sale system; or (2) by tapping it against a point of sale device's contactless reader. Visit http://www.emv-connection.com/ for more information on EMV.

2.16   **"EMV Transaction"** means the electronic acceptance of an EMV Card's chip data by point of sale equipment or other electronic payment device at the time of Sale, and the inclusion of that data with the electronic submission of the Sale. Only a "Card Swipe", "EMV Transaction" or its manual equivalent, an "Imprint", is acceptable by the Card Scheme as proof that the Card was present at the time of the Sale.

2.17   **"HPS"** means collectively Heartland Payment Systems, Inc., and its sponsoring banks, and other vendors and subcontractors.

2.18   **"Member Sponsor Bank"** is a bank that has obtained a membership with the Card Brands to allow processor access to the Card Brand Networks.

2.19   **"Merchant"** generally means the party identified as the recipient of this Agreement. It can cover the merchant itself and any third party that may be associated with them (i.e. VARs, gateway providers etc.).

2.20   **"MCC"** also known as **"Merchant Category Code"** is a 4 digit number used to describe the Merchants primary business.

2.21   **"Outbound Telemarketing Transaction"** means a transaction in which a sale of products or services results from a Merchant-initiated contact with a Cardholder via a telephone call, or a mailing (other than a catalog) that instructs the Cardholder to call the Merchant.

2.22   **"Pass Through"** means charging the Merchant the precise amount of monies designated as Interchange, Costs, Dues, Assessments and Fees as per the Card Schemes. Pass Thru or Pass Through means no mark-ups are taken by the Payment Processor or any other party when Interchange, Dues, Fees, Costs and Assessments are collected from the Merchant.

2.23   **"Payment Facilitator"** is a merchant of record who facilitates transactions on behalf of a sub-merchant whose volume is less than USD 100,000 in MasterCard and Maestro volume combined.

2.24   **"Payment Service Provider (PSP)"** is an entity contracting with a Visa, Discover or American Express member to provide payment services to sponsored merchants. The new term PSP replaces the old terminology IPSP which now includes all commerce type aggregation, including face-to-face in addition to ecommerce merchant aggregation.

2.25   **"Products"** means all goods and payment services that are sold or offered by the Merchant.

2.26   **"Rules"** means the operating regulations, requirements terms and conditions of the Card Schemes presently in effect and as they may be amended from time to time.

2.27   **"Sales Draft"** means an electronic receipt evidencing a sales Transaction.

2.28   **"Sub-merchant"** is a customer conducting business through a Third Party relationship acting as a Payment Facilitator (PF) or Payment Service Provider (PSP).

2.29   **"Third Party Agent (TPA)"** means entities that have been engaged by a Merchant or a member to perform contracted services on behalf of that Merchant or member, including value add resellers (VARs) and payment gateway providers.

2.30   **"Transaction"** means any retail sale of Products or Services, or credit therefore, from a Merchant for which the customer makes payment using any Card presented to HPS for payment.

2.31   **"Virtual Terminal"** means a credit Card processing equipment on a secure server on the Internet whereby Merchant can key enter credit Card Transactions manually.

2.32   **"Voice Authorization"** means an Authorization obtained by a direct-dialed telephone call.

2.33   **"Web Payment Solution"** may be used interchangeably with "Heartland/TouchNet Hosted Website" and means an automated solution that will allow Cardholders to pay a Merchant on a hosted website.

3. Data Security Requirements

3.1   The PCI Security Standards Council ("PCI SSC") was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa, Inc. All five founders agreed to incorporate PCI Data Security Standards ("PCI DSS") as the technical requirements of each of their data security compliance programs. The PCI SSC is responsible for the Payment Application Data Security Standard ("PA-DSS") and PIN Transaction Security Requirements for PIN-Entry Devices ("PED").

More information, including the complete PCI DSS specifications can be found at www.pcisecuritystandards.org.

Each of the Card Schemes has requirements based on PCI DSS that define a standard of due care and enforcement for protecting sensitive information. Merchant must meet the compliance validation requirements defined by the Card Schemes available at:
www.visa.com/cisp
www.mastercard.com/sdp
www.discovernetwork.com/fraudsecurity/disc.html
www.americanexpress.com/datasecurity - For American Express Direct Merchants Only.

The Card Schemes or HPS may levy fines, suspend or terminate services, or impose other restrictions if it is determined that Merchant is not compliant with applicable security standards. Merchant is responsible for all fines and fees assessed by any Card Scheme in connection with violation of data security standards.

4. Rights, Duties, and Responsibilities of Merchants

4.1   Merchant agrees that during the term of this Agreement HPS/TouchNet shall be the primary provider for all payment processing services provided hereunder.

4.2   Merchant's policy for the adjustment of payment rendered shall be disclosed to the Cardholder before a Card sale is made. If Merchant does not make these disclosures, a full refund in the form of a credit to the Cardholder's Card account must be given. In no circumstances shall any cash refunds be given on any item originally charged to a card.

4.3   MERCHANT ACKNOWLEDGES THAT AN AUTHORIZATION DOES NOT CONSTITUTE (A) A WARRANTY THAT THE PERSON PRESENTING THE CARD

IS THE RIGHTFUL CARDHOLDER, OR (B) A PROMISE OR GUARANTEE BY HPS THAT IT WILL PAY OR ARRANGE FOR PAYMENT TO MERCHANT FOR THE AUTHORIZED TRANSACTION. AN AUTHORIZATION DOES NOT PREVENT A SUBSEQUENT CHARGEBACK OF AN AUTHORIZED TRANSACTION PURSUANT TO THIS AGREEMENT.

4.4   Merchant shall at all times maintain a direct deposit account (the "Account" or "DDA"), in good standing, at a bank that is a Receiving Depository Financial Institution (RDFI) of the Federal Reserve Bank ACH System or other ACH settlement network. Merchant agrees that all credits for collected funds shall be made automatically to the Account. Merchant also agrees that it is responsible for all fines, fees, Chargebacks, Credit Vouchers, payments and adjustments and other amounts due under the terms of this Agreement (including but not limited to attorneys fees and early termination charges) which shall be automatically made to the Account. Merchant shall not close, restrict or change the Account without prior written approval from HPS. Merchant agrees to pay HPS a twenty-five dollar ($25.00) fee on all returned ACH items. Merchant is solely liable for all fees and all overdrafts, regardless of cause. HPS shall have the unlimited right to debit without prior notice, any Account containing funds for the purpose of satisfying any liability incurred on behalf of Merchant.

4.5   Merchant shall not deposit any Transaction for the purpose of obtaining or providing a cash advance, or make a cash disbursement to any other Cardholder (including Merchant when acting as a Cardholder), or receive monies from a Cardholder and subsequently prepare a credit to Cardholder's account.

4.6   As partial consideration for this Agreement, Merchant expressly authorizes HPS to change the Member Sponsor Bank providing settlement services to Merchant. Merchant agrees to execute all necessary documents enabling HPS to effect such change, as may be required by HPS.

4.7   Intentionally Removed

4.8   Merchant shall give HPS immediate written notice of any complaint, subpoena, Civil Investigative Demand or other process issued by any state or federal governmental entity that alleges, refers or relates to any illegal or improper conduct of Merchant. Failure to give such notice shall be deemed to be a material breach of this Agreement.

4.9   Merchant shall not be assessed a Chargeback Fee for the first three Chargeback requests processed in any twelve month period beginning with the Merchant's anniversary date. Once three Chargeback requests have been submitted by the Card Scheme or Bank in any such 12 month period, HPS shall bill the Chargeback Fee applicable at that time. For purposes of this Section 4.9, the anniversary date shall be the date of Merchant's first deposit with HPS unless otherwise designated by HPS.

4.10   Merchant shall ensure HPS has the correct business taxpayer ID ("TIN") and legal name on file for Form 1099-K tax reporting purposes. Any merchant reporting an invalid TIN

and legal name combination is subject to backup withholding of an amount as defined by applicable state tax and IRS regulations.

4.11   Merchant shall at all times comply with the Rules and operating regulations of each of the Card Schemes and American Express as well as all applicable federal, state, and local, rules and regulations. Moreover, in the event of Merchant's non-compliance, Merchant accepts the responsibility for the payment of any and all fees and penalties levied because of its non-compliance.

4.12   Merchant agrees that it will not knowingly introduce into HPS' System any virus, "time bomb", or any other contaminant, including but not limited to, codes, commands, or instructions that could damage or disable HPS' System or property.

4.13   Merchant shall assume responsibility for managing the repair of problems associated with Merchant's own telecommunications and processing system (both hardware and software), including terminals.

4.14   MSP/TPA/PSP/PF must comply with all Rules as set forth in this Agreement and the following websites:

•http://usa.visa.com/merchants/risk_management/thirdparty_agents.html
•http://www.mastercard.com/us/merchant/pdf/BMEntire_Manual_public.pdf

4.15   Payment Service Provider (PSP)/ Payment Facilitator
(PF) agrees to promptly disclose to their Sub-merchant any new or increased Card Scheme related Dues, Assessments and Fees, including but not limited to Convenience fees, in accordance to the contracted services performed by the Merchant.

4.16   Merchant must meet requirements as defined by the Card Schemes. Information is available at:
www.visa.com
www.mastercard.com
www.discovernetwork.com
www.americanexpress.com/merchantopguide - For American Express OptBlue Program Merchants Only.
www.americanexpress.com - For American Express Direct Merchants Only.

5. Debit Card Processing

5.1   Merchant understands and agrees that HPS and Bay Bank, FSB or any other bank to which this agreement is assigned is a sponsored affiliate or member of each debit network and HPS is a service provider for processing Merchant's debit card Transactions pursuant to the terms herein.

5.2   Any claims Merchant may have regarding Debit services may not be offset against Bankcard sales.

5.3   Debit transactions are governed by network regulations as well as federal and state laws and regulations, including but not limited to the Electronic Funds Transfer Act, and Regulation E, pursuant to which consumers may have up to sixty (60) days to dispute a Transaction. Merchant shall comply with all applicable federal, state and local laws and regulations.

6. Fees

6.1   HPS may amend the Fees set forth in the Merchant Application as follows: If Convenience Fees are fixed, then HPS may amend such Fees if (i) any Card Scheme or third party changes its fees with HPS or (ii) the average ticket size increases from the average ticket size of the previous thirty (30) day period. If Convenience Fees are percentage-based, then HPS will only amend such Fees if any Card Scheme or third party changes its fees with HPS. The amended Fees shall be effective on the date specified in a written notice thereof, which date shall not be fewer than fifteen (15) days after the date of notice. Merchant shall attach each such revised Schedule of Fees, or written notice to the Merchant's copy of this Agreement.

6.2   Merchant shall pay all applicable sales taxes for services and products provided by HPS.

6.3   Merchant shall pay such fees and charges as may be set by HPS for any requested system enhancements or services in addition to those specified herein or in the Application or as may be requested by applicable law or changes in Card Scheme Rules.

7. Rights, Duties and Responsibilities of HPS

7.1   Merchant acknowledges that HPS may provide payment transaction processing services hereunder through contracts or subcontracts with third parties engaged in the business of transaction processing and authorizations, and specifically authorizes such third parties to exercise all of the rights of HPS hereunder. Upon request in writing by Merchant, HPS will identify the third parties involved in Merchant's processing.

7.2   HPS may, through its performance of the Services, provide Merchant with access to equipment and other hardware, software, including interface applications, processes and other such tangible or intangible property of HPS. HPS retains all ownership rights to such property and does not provide any license or any other use other than as specifically set forth herein.

7.3   HPS will accept all Sales Drafts deposited by Merchant that comply with the terms of this Agreement. HPS will pay to Merchant the total face amount of each Sales Draft, less any Credit Vouchers, or adjustments determined. All payments, credits and charges are

subject to audit and final review by HPS and prompt adjustment shall be made as required. Notwithstanding any other provision in this Agreement, HPS may refuse to accept any Sales Draft, revoke its prior acceptance, or delay processing of any Sales Draft for any reasonable period of time, as HPS deems necessary and appropriate. HPS shall have no liability to Merchant for additional charges, higher rates, or any other loss, expense or damage Merchant may incur directly or indirectly due to any such refusal, revocation or delay.

7.4   HPS will accept all customer service calls and other communications from Merchant, relating to the services provided under this Agreement including, but not limited to, equipment service, disbursement of funds, account charges, Merchant statements and Chargebacks. Merchant waives any claim relating to amounts charged to Merchant or amounts paid to unless presented within forty-five (45) days of statement date.

7.5   HPS will process all requests for Sales Drafts and Chargebacks from Card Issuers and will provide Merchant with prompt notice of requests and Chargebacks.

8. Chargebacks

8.1   Merchant agrees to pay HPS the actual amount of any Transaction processed by HPS pursuant to this Agreement whenever any Card or Debit Transaction is reversed.

8.2   Merchant agrees to pay HPS any fees or fines imposed on HPS resulting from Chargebacks and any other fees or fines imposed with respect to or resulting from acts or omissions of Merchant.

8.3   HPS agrees to mail or electronically transmit all Chargeback documentation to Merchant promptly at Merchant's address shown in the Application. Merchant is responsible for verifying its monthly statement and its daily deposit for Chargebacks and Chargeback handling fees pursuant to this Agreement. Merchant shall notify HPS in writing within forty-five (45) days after any debit or credit is or should have been affected. If Merchant notifies HPS after such time, HPS shall not have any obligation to investigate or effect any such adjustments. Any voluntary efforts by HPS to assist Merchant in investigating such matters after the 45 day notification has expired, shall not create an obligation to continue such investigation or any future investigation. Merchant must provide all information requested by HPS by the time specified in a request for information; failure to do so shall constitute a waiver by Merchant of its ability to dispute or reverse a Chargeback or other debit, and Merchant shall be solely responsible. If HPS elects, in its sole discretion, to take action on a Chargeback or other debit after the time specified to respond has expired, Merchant agrees to pay all costs incurred by HPS. Merchant agrees to pay HPS a processing fee for Sales Draft retrieval requests at HPS discretion.

9. Limitation of Liability: Due Care

9.1   Except as provided in section 9.4 hereof, HPS's sole liability to Merchant hereunder shall be to correct, to the extent reasonably practical, errors that have been caused by HPS, except that any claim by the Merchant relating to statement accuracy or amounts owed by HPS to the Merchant is waived unless presented within forty-five (45) days of statement date.

9.2   No claim for damages for any performance or failure of performance by HPS under this Agreement shall exceed the Convenience Fee amount and any other fees or charges paid to HPS in connection with the Card Transaction that is the subject of the alleged failure of performance.

9.3   IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR SPECIAL, CONSEQUENTIAL, INDIRECT, OR EXEMPLARY DAMAGES, INCLUDING LOST PROFITS, REVENUES, AND BUSINESS OPPORTUNITIES. THE PROVISIONS OF THIS PARAGRAPH SHALL SURVIVE THE TERMINATION OF THIS AGREEMENT. Without limitation of the foregoing, HPS shall not be liable to Merchant for delays in data transmission. Merchant acknowledges that any losses pursuant to this Agreement are commercial in nature.

9.4   HPS MAKES NO WARRANTY WHATSOEVER REGARDING CARD AUTHORIZATIONS, DECLINES OR REFERRAL CODES, RESPONSES TO REQUESTS FOR AUTHORIZATION, PROCESSING, SETTLEMENT, OR ANY OTHER SERVICES PROVIDED BY OR ON BEHALF OF HPS HEREUNDER, AND HPS HEREBY DISCLAIMS ANY AND ALL SUCH WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE, and HPS shall have no liability to Merchant or any other person for any loss, liability or damage arising directly or indirectly in connection herewith. Without limitation of the foregoing, Merchant acknowledges that HPS has no liability or responsibility for the actions of any Card Scheme, Card Issuer or Cardholder.

9.5   Neither Party shall be liable for delays in processing or other non-performance caused by such events as fires; telecommunications failures; equipment failures; strikes; riots; war; non-performance of vendors, suppliers, processors or transmitters of information; acts of God or any other causes over which the Party has no control.

10. Display of Materials: Trademarks

10.1   If permissible under state law, Merchant agrees to prominently display the promotional materials provided by HPS in its place(s) of business or on an eCommerce site whereby Card Scheme logos must prominently be displayed. Use of promotional materials and use of any trade name, trademark, service mark or logo type ("Marks") associated with

Card(s) shall fully comply with specifications contained in applicable Card Scheme operating regulations.

10.2   Merchant shall not use any promotional materials or Marks in any way that suggests or implies that a Card Scheme endorses Merchant's products or services.

10.3   Merchant agrees that it will discontinue use of any Mark of a Card Scheme wherever such Marks are displayed, including on the Merchant's website(s), once (a) the Agreement is terminated or expires or (b) Merchant discontinues acceptance of a Card or participation in a Card Scheme Program.

11. Term: Termination

11.1   This Agreement shall become effective upon acceptance of the first Merchant deposit by HPS and shall continue in effect for a term of sixty (60)   months therefrom. Thereafter, the Agreement will automatically renew for additional twelve (12) month periods unless terminated by any party by giving ninety (90) days written notice prior to the end of any term, except that in case of an Event of Default by Merchant or as required by a Card Scheme, this Agreement may be terminated by HPS immediately, and HPS shall give Merchant written notice within ten (10) days thereafter.

11.2   In the event HPS fails to provide the Services as stated herein, prior to exercising any right of termination, Merchant must (i) notify HPS of such breach; (ii) give HPS a reasonable period to cure, depending on the nature of the breach. The parties shall agree on the duration of such reasonable period in writing; and if, HPS is unable to cure within such time, Merchant may terminate the Agreement subject to the terms herein.

11.3   If any of the following events shall occur (each an "Event of Default"):
   (i)   Merchant shall default in any material respect   in the performance or observance of any term, covenant, condition or agreement contained in this Agreement; or
   (ii)   A reasonable belief by HPS that Merchant will constitute a risk to HPS by failing to meet the terms of this Agreement; or
   (iii) Material adverse change in the business, financial condition, business procedure or services of Merchant; or
   (iv)   any information contained in the Application was or is incorrect in any material respect, is incomplete or omits any information necessary to make such information and statements not misleading to HPS; or

   (v)   irregular Card sales or credits by Merchant, Card sales substantially greater than the average ticket amount stated on Merchant's Application, excessive Chargebacks or any other circumstances which in the sole discretion of HPS, may increase the risk of Merchant Chargebacks or otherwise present a financial or security risk to HPS; or

(vi) reasonable belief by HPS that Merchant is engaged in practices that involve elements of fraud or conduct deemed to be injurious to Cardholders, including, but not limited to fraudulent, prohibited or restricted Transaction(s); or

(vii) any voluntary or involuntary bankruptcy or insolvency proceedings involving Merchant, its parent or an affiliated entity, or any other condition that would cause HPS to deem Merchant to be financially insecure; or

(viii) Merchants engages in any Outbound Telemarketing Transactions; or

(ix) Merchant or any other person owning or controlling Merchant's business is or becomes listed in any Card Scheme's security reporting;

Then, upon the occurrence of any Event of Default, all amounts payable hereunder by Merchant to HPS shall be immediately due and payable in full.

11.4   In the event of termination, regardless of cause, Merchant agrees that (a) all obligations and liabilities of Merchant with respect to any Sales Draft or Credit Voucher presented prior to the effective date of termination shall survive such termination and expressly authorizes HPS to withhold and discontinue the deposit to Merchant's Account for all Card and other payment transactions of Merchant in the process of being collected and deposited; and (b) it will discontinue all use of Marks of a Card Scheme or HPS.

11.5   Merchant agrees that all obligations incurred or existing under the terms of this Agreement as of the date of termination, shall survive such termination. After the termination or expiration of the terms of the agreement, Client shall discontinue using and shall remove all hyperlinks, signs, displays or other materials containing the name or logo of HPS/TouchNet and/or its suppliers.

11.6   Neither the expiration nor termination of this Agreement shall terminate the obligations, or rights of the parties pursuant to provisions of the Agreement, which by their terms are intended to survive or be perpetual or irrevocable.

11.7   If any Event of Default shall have occurred and be continuing, HPS may, in its sole discretion, exercise all of its rights and remedies under in equity, contract or applicable law, including, without limitation, those provided in this Agreement.

11.8   The provisions governing processing and settlement of Card Transactions, all related adjustments, fees and other amounts due from Merchant and the resolution of any related Chargebacks, will continue to apply after termination of this Agreement until all Card Transactions made prior to such termination are settled or resolved. Upon termination of this Agreement, Merchant agrees to promptly send HPS all data relating to Card Transactions made to the date of termination.

12. Terminated Merchant File

12.1   If Merchant is terminated for any of the reasons specified as cause by Visa, MasterCard and Discover Network, HPS may report Merchant's business name and the names and

other identification of its principals to the Terminated Merchant File. Merchant expressly agrees and consents to such reporting, and HPS shall have no liability to Merchant for any loss, expense or damage Merchant may sustain directly or indirectly due to such reporting.

13. Notices

13.1   All notices and other communication required or permitted under this Agreement shall be deemed delivered when mailed first-class mail, postage prepaid, addressed to the Merchant at the address stated in the Application and to HPS at the address set forth below, or at such other address as the receiving party may have provided by written notice to the other:

Heartland Payment Systems
Attn: Customer Care
One Heartland Way
Jeffersonville, IN. 47130
1 (888) 963-3600

Member Bank Sponsors

Issues Regarding Credit Cards
Barclay Bank
125 South West Street
Wilmington, DE 19801
Phone #: 1 (201) 622-8990
The Bancorp Bank
409 Silverside Road, Suite 105
Wilmington, DE 19809
Ph #: 1 (302) 385-5000

Wells Fargo Bank, N.A.
1200 Montego
Walnut Creek, CA 94598
Phone #: 1 (925) 746-4167

Issues Regarding Debit Cards
Bay Bank
7151 Columbia Gateway Drive
Suite A
Columbia, MD 21046

14. Additional Terms

14.1   Truth of Statements: Merchant represents to HPS that all information and all statements contained in the Application are true and complete and do not omit any information necessary to make such information and statements not misleading to HPS.

14.2   Entire Agreement: This Agreement constitutes the entire understanding of HPS and Merchant and supersedes all prior agreements, understanding, representations, and negotiations, whether oral or written between them.

14.3   Amendments: Except as otherwise provided herein, no provision of this Agreement may be waived, amended or modified except in writing signed by an authorized representative of each party.

14.4   No Waiver of Rights: Any failure of a Party hereto to enforce any of the terms, conditions or covenants of this Agreement shall not constitute a waiver of any rights under this Agreement.

14.5   Section Headings: All section headings contained herein are for descriptive purposes only, and the language of such section shall control.

14.6   Assignability: Neither Party hereto may assign this Agreement directly or by operation of law, without the prior written consent of the non-assigning party, which consent shall not be unreasonably withheld, Either party may assign this Agreement to a parent, subsidiary, or affiliate without the other's consent.   This Agreement shall be binding upon the parties hereto, their successors and permitted assigns.   Any assignment without the prior written consent of the non-assigning party shall be void.

14.7   Damages: In any judicial or arbitration proceedings arising out of or relating to this Agreement, including but not limited to these actions or proceedings related to the collection of amounts due from merchant, the providing party shall recover, in addition to all damages awarded, all court costs, fees and expenses of experts.

14.8   Relationship of the Parties: Nothing contained herein shall be deemed to create a partnership, joint venture or, except as expressly set forth herein, any agency relationship between HPS and Merchant.

14.9   Severability: If the performance by either party of any provision of this Agreement is determined to be unlawful or in violation of any state, federal or local statute, law, ordinance, regulation or rule, or of the rules of any Card Scheme, said party shall seek to cure the illegality or violation within thirty (30) days following the date that such party is first informed of such violation or illegality.   If such cure is not affected within such thirty (30) days period, the illegal or violating provision shall be null and void, and this Agreement shall remain in full force and effect and the parties shall use their best efforts to agree upon legal and non-violating substituted provisions that will serve the intent of the parties.

14.10 **Privacy Policy:** All financial and personal information about Merchant and a Merchant's vendors and suppliers, is considered confidential data. Merchant acknowledges and agrees that this information or other personal information will be used only in connection with the services provided by HPS and third parties designated by HPS to Merchant under the terms of this agreement and the performance of this Agreement. Notwithstanding the foregoing or anything else contained herein, Merchant information may be provided by HPS to any third party including but not limited to, Card Schemes, collection agencies, financial institutions or organizations, or merchant associations in the event of a default by merchant in any obligation under this agreement.

14.11 **Governing Law:** This Agreement shall be construed and governed by the laws of the state of in which the government or public educational entity is located without regard to legal principles related to conflict of laws.

14.12 **Jurisdiction & Venue:** Any suit, action or proceeding (collectively "action") arising out of or relating to this Agreement shall be brought only in the courts of the state of which the government or public educational entity is located or in the applicable United States District Court. The parties hereto agree and consent to the personal and exclusive jurisdiction of said courts over them as to all such actions, and further waive any claim that such action is brought in an improper or inconvenient forum. In any such action, the parties waive trial by jury.

14.13 **No Third Party Beneficiary.** Under no circumstance, shall any third party be considered a third party beneficiary of Merchant's rights or remedies under this Agreement or otherwise be entitled to any rights or remedies of Merchant under this Agreement.

14.14 **Changes:** HPS may change the terms of or add new terms to this Agreement at any time in accordance with applicable law. Any such changes or new terms shall be effective when notice thereof is given by HPS either through written communication or on its merchant website located at https://infocentral.heartlandpaymentsystems.com.

14.15 **Public Statements.** Merchant shall obtain the prior written consent of HPS prior to making any written or oral public disclosure or announcement, whether in the form of a press release or otherwise, which directly or indirectly refers to HPS.

15. Optional Card Brand Fees:

Convenience Fee: A fee charged to the Cardholder by the Merchant for a true convenience for accepting a credit or debit card. Examples of a "true convenience" are payment through the internet, mail order or phone order. All Card Schemes allow Merchants to charge a convenience fee. All Card Schemes must be charged equally. The Merchant is required to disclose the fee to the Cardholder and provide the Cardholder with the opportunity to cancel the Transaction, if the Cardholder does not want to pay the convenience fee. In addition to the foregoing, (i) Visa requires Merchants to have a brick

14 | 01/23/2017

and mortar location in order to be allowed to charge a convenience fee; (ii) MasterCard requires processors to register any Government or Education merchant; and (iii) AMEX requires that the convenience fee be shown as a separate charge on the Cardholder's receipt for the goods or services.

Surcharge: A charge in addition to the initial amount of the sale on a credit card to cover the Merchant's cost of acceptance. All Card Schemes allow surcharging. Visa, MasterCard and Discover require Merchants to register with the Card Schemes. The Merchant is required to disclose the fee at the entry of their establishment and at the point of sale. The cardholder must be given the opportunity to cancel the Transaction if they do not want to pay the surcharge fee. The amount of the charge cannot exceed the amount of the Merchant's discount fee on Visa, MasterCard and Discover and is capped at 4%. The surcharge must appear on the sales receipt separately from the sales amount. All Card Schemes must be charged equally. Currently there are several states that prohibit surcharging. Merchants should check their state and local laws prior to initiating a surcharge.

Service Fee: Visa allows government and education Merchants to charge a different type of fee called a "service fee". This fee is assessed for accepting payments for taxes, fees and fines for government MCCs and for tuition, room and board, lunch programs, etc. for education MCC Merchants. The service fee can be charged on credit and debit Transactions, in a face-to-face or card not present environment. The service fee must appear separate from the sales amount on the receipt. Merchants must be registered through Visa. Service fee must be disclosed prior to completion of the transaction, allowing the cardholder to cancel the Transaction if they do not wish to accept the service fee. MasterCard allows government and education merchants to charge "convenience fees" and has no separate "service fee" for these MCCs.

Other Fees: Handling fees and payment fees are allowed on all Card Schemes as long as these fees are charged on all payment channels; cash, checks, ACH, etc. These are not governed by the Card Schemes specifically. State and local laws may apply and merchants should ensure the fees are allowed in their area of business.

Revised: 02/19/16

15 | 01/23/2017

EXHIBIT C

Visa Core Rules and
Visa Product and Service Rules

18 April 2020

Version 1.1 (4 May 2020)

© 2014—2020 Visa. All Rights Reserved.

The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other trademarks not attributed to Visa are the property of their respective owners.

Visa is committed to providing our partners and interested parties with greater insight into Visa's operations. As part of our effort, we are pleased to provide access to the latest edition of the *Visa Core Rules and Visa Product and Service Rules,* which govern participation of our financial institution clients in the Visa system.

To protect cardholders and merchants and maintain the integrity of the Visa system, we have omitted proprietary and competitive information, as well as certain details from the rules relating to the security of the network.

Any regional or country-specific rules within the *Visa Core Rules and Visa Product and Service Rules* apply only to the operations of financial clients within the relevant region or country, and any rules marked with the name of a region(s) or country(ies) are applicable to financial institutions operating in that region(s) or country(ies) only.

The Visa Rules must not be duplicated, in whole or in part, without prior written permission from Visa.

If you have questions about Visa's rules, please *contact us*.

Contents

Contents

Visa Core Rules and Visa Product and Service Rules

Contents

Visa Core Rules and Visa Product and Service Rules

Contents

Contents
Visa Core Rules and Visa Product and Service Rules

Contents

Visa Core Rules and Visa Product and Service Rules

Contents

Visa Core Rules and Visa Product and Service Rules

Contents

Visa Core Rules and Visa Product and Service Rules

Contents

Visa Core Rules and Visa Product and Service Rules

Contents

Contents

Contents
Visa Core Rules and Visa Product and Service Rules

Contents

Visa Core Rules and Visa Product and Service Rules

Contents
Visa Core Rules and Visa Product and Service Rules

Contents

Contents

Contents

Contents

Visa Core Rules and Visa Product and Service Rules

Contents
Visa Core Rules and Visa Product and Service Rules

Contents

Contents
Visa Core Rules and Visa Product and Service Rules

Contents

Contents

Contents

Visa Core Rules and Visa Product and Service Rules

Contents

Tables

Tables

Visa Core Rules and Visa Product and Service Rules

Tables

Visa Core Rules and Visa Product and Service Rules

Tables
Visa Core Rules and Visa Product and Service Rules

Tables
Visa Core Rules and Visa Product and Service Rules

Tables

Visa Core Rules and Visa Product and Service Rules

Tables

Visa Core Rules and Visa Product and Service Rules

Tables

Tables

Visa Core Rules and Visa Product and Service Rules

Tables

Visa Core Rules and Visa Product and Service Rules

Tables

Visa Core Rules and Visa Product and Service Rules

Tables

Visa Core Rules and Visa Product and Service Rules

Summary of Changes

Summary of Changes Since the 19 October 2019 Visa Core Rules and Visa Product and Service Rules

Change
4 May 2020 Minor Revision   A minor language correction has been made with no change to the intent of the rule.
Glossary Terms Updated   A number of glossary terms in the Visa Rules have been updated and expanded to reflect the current payment environment and achieve clearer communication and more streamlined rules.
Updates to Visa Easy Payment Service (VEPS) Limits and Floor Limits   **Effective 19 March 2020, 17 July 2020, and 16 October 2020**   In the AP Region (Philippines), Europe Region (Belgium, Poland): Updates have been made to the maximum Transaction amounts for Visa Easy Payment Service (VEPS) Transactions.   **Effective 10 April 2020 and 16 October 2020**   In the CEMEA Region (Albania, Armenia, Azerbaijan, Bahrain, Belarus, Bosnia and Herzegovina, Egypt, Georgia, Kazakhstan, Kosovo, Kuwait, Kyrgyzstan, Lebanon, Moldova, Montenegro, Morocco, North Macedonia, Pakistan, Qatar, Saudi Arabia, Serbia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan): Updates have been made to the maximum Transaction amounts for Visa Easy Payment Service (VEPS) Transactions.   **Effective 17 October 2020**   In the AP Region (Philippines): Updates have been made to the Floor Limit.
BIN Attribute Disclosure Clarifications   **Effective 23 January 2020**   Revisions have been made to clarify what BIN Attributes are and how, when, and with whom they may be shared.
Consolidation of Stop Payment Service Rules   **Effective 17 August 2020 in the Europe Region, and effective 19 October 2020 in the AP Region, Canada Region, CEMEA Region, LAC Region, and US Region**   The Visa Stop Payment Service will launch globally, replacing both the Visa Europe Payment Stop Service and the Pre-authorized Payment Cancellation Service.

Summary of Changes

Visa Core Rules and Visa Product and Service Rules

Change
Account Funding Transaction Requirements   **Effective 18 April 2020**   Revisions have been made to clarify Account Funding Transaction requirements and classify the *Account Funding Transaction (AFT): Processing Guide* as a Visa Supplemental Requirement.
Sunset of Multinational Merchant Acceptance Program (MMAP)   **Effective 17 October 2019**   New enrollments in the Multinational Merchant Acceptance Program (MMAP) will be discontinued temporarily.
Amendments to Installments, Prepayments and Stored Credentials Rules   **Effective 25 January 2020**   Acceptance policies have been expanded for installments on Visa cards, when the installment provider is neither the card issuer nor the seller of the goods or services. Additionally, existing Debt repayment, Stored Credential, and prepayment Transaction requirements have been streamlined.
Enhancement of High-Brand Risk Acquiring Rules   **Effective 17 April 2020 and 16 October 2020**   The list of High-Brand Risk Merchants and various requirements for Acquirers of High-Brand Risk Merchants have been updated.
Updates to Credit Transaction Requirements for Mass Transit Operators   **Effective 18 April 2020**   Revisions have been made to the rules related to Merchant processing of credits to Cardholders. The requirement to authorize a Credit Transaction is now optional for mass transit merchants globally.
New Investigation Fees and What To Do If Compromised Update   **Effective 19 October 2019**   Updates have been made to Visa's What To Do If Compromised (WTDIC) document and new investigation fees and non-compliance assessments are being introduced.
ATM Adjustment Processing Conditions   **Effective 18 April 2020**   Revisions have been made to limit to 2 the maximum number of ATM Adjustments submitted by an Acquirer

Visa Core Rules and Visa Product and Service Rules

Change
if the Adjustments result from ATM Reversals processed with certain reason codes on the same Account Number and the same Transaction Date.
Visa Digital Commerce Program (VDCP) Participation Requirements for Acquirers **Effective 18 April 2020** Revisions have been made to incorporate key provisions of the Visa Digital Commerce Program (VDCP) agreement into the Visa Rules to simplify implementation of the program for Acquirers choosing to participate.
Updates to Requirements for Card Vendor Envelopes **Effective 18 April 2020** Revisions have been made to remove the prohibition against an Issuer identifying itself on envelopes which contain Visa Products. The Issuer will have the option to use either a nondescript envelope or include similar markings as included on other Issuer or Affinity/Co-Brand communications.
Miscellaneous Dispute Rule Revisions **Effective 20 April 2020 and 17 October 2020** Revisions were made to the Dispute rule language for clarity and consistency, and to remove obsolete rules.
Expansion of Contactless-Only Acceptance to Additional Segments, Environments, and Countries **Effective 18 April 2020 and 17 April 2021** Revisions have been made to expand the allowance for Merchant Outlets to deploy Contactless-only Acceptance Devices.
Clarifications to Processing Requirements for Processing Integrity and Duplicate Correction **Effective 17 April 2021** Revisions have been made to clarify processing requirements for Authorization Reversals and Clearing Reversals.
Review of Non-Compliance Assessments (NCAs) **Effective 18 April 2020** Revisions have been made to review the non-compliance assessments to remove non-active programs and map some schedules with the General Schedule. In addition the Global Brand Protection Program has been updated to group all categories in the program to use one schedule.
Increases to Automated Fuel Dispenser (AFD) Status Check Authorization Limits

Change
Effective 17 October 2020 Revisions have been made to increase Status Check Authorization limits for Automated Fuel Dispenser (AFD) Transactions acquired by fuel Merchants in the US Region.
Revisions to Cardholder Authentication Verification Value (CAVV) Requirements for EMV 3-D Secure Transactions **Effective 17 October 2020 in the Canada Region, Europe Region, LAC Region, US Region, and effective 17 April 2021 in the AP Region, CEMEA Region** Revisions have been made to Cardholder Authentication Verification Value (CAVV) Requirements for EMV 3-D Secure Transactions.
Agent-Related Definition and Rule Updates **Effective 12 December 2019** Revisions have been made to expand the definition of Third Party Agent.
First Party Fraud Rules Expansion – AP Region **Effective 18 April 2020** First party fraud rules are being expanded to the AP region.
Updates to Required Use of VisaNet for Processing – AP Region (Bangladesh) **Effective 18 April 2020** In the AP Region (Bangladesh): Revisions have been made to require the use of VisaNet for authorizing, clearing, and settling of all Domestic POS transactions.
Use of Visa Secure with 3D Secure 2.0 – AP Region (Cambodia) **Effective 18 April 2020** In the AP Region (Cambodia): Revisions have been made to require Members to support Visa Secure with 3-D Secure 2.0.
Changes to Processing Timeframes for Domestic Transactions – AP Region (India) **Effective 1 November 2019** In the AP Region (India): Revisions have been made to decrease Acquirer processing time frames for Domestic Transactions and Issuer holds on funds in Payment Credential Users' accounts.
Updates to Visa UHNW Product Requirements – AP Region (Singapore)

Visa Core Rules and Visa Product and Service Rules

Change
Effective 25 January 2020
In the AP Region (Singapore): Revisions have been made to Visa Ultra High Net Worth product requirements, including an updated minimum spend requirement and a new requirement for maximum issuance.
Payment Facilitators, Acquirer Direct Merchant Agreement Limit – AP Region (Taiwan)
Effective 19 October 2019
In the AP Region (Taiwan): The annual Transaction volume limit has been revised at which an Acquirer must establish a direct agreement with a Sponsored Merchant.
Use of Visa Secure with 3D Secure 2.0 – AP Region (Taiwan)
Effective 17 October 2020
In the AP Region (Taiwan): Revisions have been made to require Issuers to support Visa Secure with 3-D Secure 2.0.
Effective 16 January 2021
In the AP Region (Taiwan): Revisions have been made to require Acquirers to support Visa Secure with 3-D Secure 2.0.
Optional Signature Capture at Merchants with EMV-enabled Terminals – AP Region (Japan, Philippines)
Effective 18 April 2020
In the AP Region (Japan, Philippines): For EMV-enabled terminals, eligible Merchants can choose to no longer capture a signature as a form of Cardholder Verification, for any Transaction amount.
Amendments to Visa Infinite Privilege Cardholder Qualification Criteria – Canada Region
Effective 25 January 2020
In the Canada Region: Revisions have been made to expand the cardholder qualification criteria for Visa Infinite Privilege by adding "declared minimum personal income" as an option to qualify prospective cardholders .
Updates to Obligation to Comply with the Code of Conduct – Canada Region
Effective 1 February 2020
In the Canada Region: Revisions have been made to remove the Merchant Agreement Disclosure and Cancellation Rights rule to support and ensure compliance with the requirements of the Code.
New Segment for Service Fee Assessment Requirements – Canada Region

Change
Effective 9 October 2019 In the Canada Region: A new segment, Long Term Care (MCC 8050 Nursing and Personal Care Facilities) has been included in the list of segments of the Service Program.
Updates to Mass Transit Transaction Requirements – Canada Region **Effective 18 July 2020** In the Canada Region: Revisions have been made to increase the maximum Transaction amount that can be cleared following the first Decline Response.
Updates to Domestic Visa Easy Payment Service (VEPS) Limit – Canada Region **Effective 6 April 2020** In the Canada Region: Updates have been made to the maximum Transaction amount for domestic Visa Easy Payment Service (VEPS) Transactions.
First Party Fraud Rules Expansion – CEMEA Region **Effective 18 July 2020** First party fraud rules are being expanded to the CEMEA region.
Updates to Visa Rewards Minimum Requirements – CEMEA Region (Belarus) **Effective 18 April 2020** In the CEMEA Region (Belarus): Minimum level of rewards and benefits for Visa Rewards programs have been changed.
Visa Infinite Business and Visa Platinum Business Launch – Europe Region **Effective 1 July 2020 and 18 July 2020** In the Europe Region: Revisions have been made to introduce Visa Infinite Business and Visa Platinum Business products.
Strong Customer Authentication Update – Europe Region **Effective 25 November 2019** In the Europe Region (European Economic Area): A new Visa Supplemental Requirement, PSD2 SCA for Remote Electronic Transactions – European Economic Area, has been introduced.
Personalization Validation Testing (PVT) Update – Europe Region **Effective 25 January 2020**

Visa Core Rules and Visa Product and Service Rules

Change
In the Europe Region: Revisions have been made to the Personalization Validation Testing (PVT) Process to include a client self-service option.
Minimum Approval Rates – Europe Region **Effective 18 April 2020** In the Europe Region: Minimum approval rates have been aligned with the global rates and new approval rates have been introduced for EMV 3-D Secure Transactions.
Introduction of Merchant Verification Value – Europe Region **Effective 17 October 2020** In the Europe Region: The use of a Merchant Verification Value (MVV) will be required for certain Transactions.
Increase in Domestic Visa Easy Payment Service Limits – Europe Region **Effective 23 March 2020, 27 March, 1 April 2020, 6 April 2020, 15 April 2020, and 21 April 2020** In the Europe Region (Belgium, Bulgaria, Croatia, Cyprus, Greece, Hungary, Iceland, Malta, Portugal, Republic of Ireland, Turkey, United Kingdom): Updates have been made to the maximum Transaction amounts for domestic Visa Easy Payment Service (VEPS) Transactions.
Cash-Back Amount Limit – Europe Region (Switzerland) **Effective 13 June 2020** In the Europe Region (Switzerland): The allowed Cash-Back Transaction amount limit has changed to be between CHF 20 – CHF 300.
Cash-Back without a Purchase – Europe Region (United Kingdom) **Effective 18 April 2020** In the Europe Region (United Kingdom): Revisions have been made to allow Cash-Back without a Purchase.
Expansion of Service Fee Assessment Requirements – LAC Region (Trinidad and Tobago) **Effective 16 January 2020** In the LAC Region (Trinidad and Tobago): Revisions have been made to allow Service Fees for government payments.
Compelling Evidence for Keyed Transactions – US Region **Effective 18 April 2020**

Visa Core Rules and Visa Product and Service Rules

Change
In the US Region: Revisions have been made that allow merchants to provide additional types of Compelling Evidence for card-present domestic key-entered transactions processed at non-chip terminals.
Bill Payment Provider Requirements – US Region **Effective 18 April 2020** In the US Region: Revisions have been made to add requirements for Bill Payment Providers (BPP)
Consumer Credit Benefit Refresh – US Region **Effective 1 Feburary 2021** In the US Region: Visa will remove Auto Rental Collision Damage Waiver (ARCDW) and Warranty Manager (WM) benefits for select Consumer Credit product platforms as Visa-funded core benefits. Issuers will be able to purchase them as Issuer-funded optional benefits after the effective date.
Discontinuation of QR Code Processing Standards – US Region **Effective 19 October 2019** In the US Region: The EMVCo-based Visa QR Code payment specifications have been discontinued. Future QR Code Transactions processed in the US Region will be treated as Card-Absent Environment Transactions.
Visa Infinite Business Launch – US Region **Effective 19 October 2019** In the US Region: Revisions have been made to support the launch of Visa Infinite Business Card.
Visa Rent Payment Program – US Region **Effective 18 April 2020** In the US Region: Revisions have been made to introduce the Visa Rent Payment Program, which allows qualifying property owners, or their qualified third party agents that process the payments, to assess a capped fee to cardholders.
Credit Products Support Fast Funds Processing – US Region **Effective 17 April 2021** In the US Region: Revisions have been made to expand the Fast Funds requirement to apply to incoming Original Credit Transactions for credit products in the US region.
Effective Date Revisions Most effective dates older than 6 months have been deleted.

Change
Editorial Changes
Editorial revisions have been made to ensure consistency and clarity and to delete obsolete or redundant language.

ID# 0030669   **Edition: Apr 2020 | Last Updated: New**

Introduction

The Visa Rules

The Visa Core Rules and Visa Product and Service Rules

Introduction to the Visa Core Rules and Visa Product and Service Rules

Visa has established rules that are designed to minimize risks and provide a common, convenient, secure, and reliable global payment experience while supporting geography-specific rules that allow for variations and unique marketplace needs. They are set and modified by Visa to support the use and advancement of Visa products and services, and represent a binding contract between Visa and each Member.

The Visa Core Rules contain fundamental rules that apply to all Visa system participants and specify the minimum requirements applicable to all Members to uphold the safety, security, soundness, integrity, and interoperability of the Visa system.

The Visa Product and Service Rules contain rules that apply to Visa system participants based on use of a product, service, the Visa-Owned Marks, VisaNet, the dispute resolution process, and other aspects of the Visa payment system. The Visa Product and Service Rules also include operational requirements related to the Visa Core Rules.

The Visa Supplemental Requirements are Visa- or third-party-administered documents or websites that contain requirements beyond the content of the *Visa Core Rules and Visa Product and Service Rules* (for example: *Visa Product Brand Standards, BASE II Clearing Services, Visa Integrated Circuit Card Specification,* Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements).

ID# 0020308	**Edition: Apr 2020 | Last Updated: Apr 2017**

Writing Conventions

The following conventions apply to the *Visa Core Rules and Visa Product and Service Rules*:

- "Visa" refers to any Visa Region, office, management, or committee.
- If the singular is used, it means the plural, and the plural means the singular. For example: "A Merchant must …" means that "All Merchants must…"
- Responsibility is assigned to a Member. For example: "A Merchant must…" means "An Acquirer must ensure that its Merchant…"

Visa Core Rules and Visa Product and Service Rules

- Capitalized words have a meaning defined in the Glossary, except for the names of some Visa products or services, which are capitalized but not defined.

- Defined terms are often combined.

ID# 0020313	Edition: Apr 2020	Last Updated: Apr 2016

Changes to the Visa Core Rules and Visa Product and Service Rules

Changes to the *Visa Core Rules and Visa Product and Service Rules* are communicated and identified as part of the "Summary of Changes" for each edition.

Unless an effective date is specified in the text for a change to the *Visa Core Rules and Visa Product and Service Rules*, all changes are effective on the publication date.

ID# 0020315	Edition: Apr 2020	Last Updated: Oct 2014

Unique Rule IDs and Additional Information

The bar below each rule contains the following information:

Information in Rule ID

ID#	A unique 7-digit identification code that includes leading zeros. This unique ID remains with each rule for the life of that rule.
Edition	The month/year of the current edition of the *Visa Core Rules and Visa Product and Service Rules*
Last Updated	The month/year in which the rule was last changed

ID# 0020316	Edition: Apr 2020	Last Updated: Oct 2015

Part 1:
Visa Core Rules

1   Visa Core Rules

1.1   General

1.1.1   Governance

1.1.1.1   Applicability of Rules

All participants in the Visa system are subject to and bound by the Visa Charter Documents and the Visa Rules, as applicable based on the nature of their participation and geography. In the event of any conflicts between the Visa Charter Documents and the Visa Rules, conflicts will be resolved in the following order of precedence:

- Visa Charter Documents
- *Visa Core Rules*
- *Visa Payment System Operating Regulations – Russia* (if applicable)
- Published domestic rules within the Europe Region (if applicable)
- *Visa International Travelers Cheque Operating Regulations* (if applicable)
- *V PAY Operating Regulations* (if applicable)
- Visa Product and Service Rules
- Visa Supplemental Requirements

Any use of or participation in any Visa services or products not covered in the Visa Rules will be governed by applicable participation agreements and associated documentation.

Previously, rules were contained in the *Visa International Operating Regulations, Visa Europe Operating Regulations,* other operating regulations or rules, extension documents, and certificates of incorporation and bylaws of various Visa entities.

The Visa Rules represent modifications and amendments to such existing Visa rules and requirements, which continue in substance and effect except as expressly modified in the Visa Rules. By reorganizing and renaming this body of requirements, Visa does not intend to modify the meaning or enforceability of any Visa published documents, forms, or contracts to which Visa is a party, or any contracts that are required by Visa to include provisions to comply with Visa's certificate of incorporation or bylaws, operating regulations, or other Visa requirements. Regardless of whether this document or other documents refer to these requirements as the *Visa International Operating Regulations* or by other prior naming conventions, such references are deemed to refer to and incorporate the Visa Rules.

Visa Core Rules and Visa Product and Service Rules

ID# 0007750   Edition: Apr 2020 | Last Updated: Apr 2018

1.1.1.2   Applicability of Processing Rules – Europe Region

In the Europe Region: A Member is not subject to or bound by processing rules in the *Visa Core Rules and Visa Product and Service Rules* where it is indicated that such processing rules do not apply to a Member.

A Member is subject to all applicable rules set out in the *Visa Europe Operating Regulations – Processing* for:

- Interregional Transactions processed through Visa systems
- Intraregional Transactions and Domestic Transactions processed through Visa systems, if the Member has elected to use Visa as its Visa Scheme Processor

ID# 0029986   Edition: Apr 2020 | Last Updated: Oct 2016

1.1.1.3   Applicable Laws and Conflicts

Each Member must comply with all applicable laws, regulations, and other legal requirements including, but not limited to, laws and regulations regarding banking, financial institutions, payment systems, foreign currency exchange, money transmission, anti-money laundering, anti-terrorist financing, sanctions (such as those administered by the US Department of the Treasury's Office of Foreign Assets Control or the Australian Government's Department of Foreign Affairs and Trade), privacy and security, consumer protection, and trademarks and copyright for each country in which the Member operates. Each Member is also responsible for ensuring that any of its affiliates, subsidiaries, parent companies, third-party agents, Merchants, and any other of its appointed agents participating in Visa's system comply with all applicable laws, regulations, and other legal requirements applicable to each country in which its affiliates, subsidiaries, parent companies, third-party agents, Merchants, and other appointed agents operate. Each Member is encouraged to consult with its own legal counsel to ensure that it is in full compliance with all applicable laws, regulations, and other legal requirements in each country in which the Member operates.

A Transaction must be legal in both the Cardholder's jurisdiction and the Merchant Outlet's jurisdiction.

In the event of any conflict between the Visa Rules and any applicable laws or regulations, the requirements of the laws or regulations govern.

ID# 0000385   Edition: Apr 2020 | Last Updated: Oct 2017

1.1.1.6   Use of the Visa Rules

The Visa Rules are only to be reviewed or used in connection with Visa payment services and must not be used, modified, copied, downloaded, transferred, or printed in part or in total for any other purpose without the express written permission of Visa.

The Visa Rules govern the relationship between Visa and its Members and their agents. The Visa Rules do not constitute a contract, promise, or representation or confer any rights, privileges, or claims of any kind as to any third parties.

Visa may amend, modify, delete, or otherwise change the Visa Rules at any time. Changes will be reflected in the next edition of the Visa Rules.

Rules that do not have a geography-specific (Visa Region or country) indication in the title or language of a rule apply to all Members unless noted otherwise. Geography-specific rules apply only to the operations of Members within the relevant geography.

ID# 0007428   **Edition: Apr 2020 | Last Updated: Oct 2014**

1.1.1.7   Restricted Use of Visa Systems and Services

Any entity that accesses or uses a Visa system and/or service must both:

- Restrict its use of the Visa system and/or service to purposes expressly approved by Visa
- Comply with Visa requirements and documentation for system and/or service access and use

ID# 0003331   **Edition: Apr 2020 | Last Updated: Oct 2017**

1.1.1.8   Provision of Updates and Support for Visa Products and Services

Effective 18 April 2020 Unless otherwise specified in the Visa Rules or agreed in a separate written agreement, Visa has no obligation to provide replacements, updates, upgrades, modifications, or any other support and maintenance for any Visa products or services.

In the event any updates are made available to Members or if Visa requires a Member to make system changes, the Member must do all of the following:

- Respond to and implement, as specified by Visa, the updates or system changes required by Visa
- Ensure that its agreements with Cardholders, Merchants, Visa-approved manufacturers, Third-Party Personalizers, and agents allow for the implementation of updates or system changes required by Visa

- Include in its agreements with Cardholders, Merchants, Visa-approved manufacturers, Third-Party Personalizers, and agents the Member's obligation to inform the contracted entity, in a timely manner, of any major updates or system changes implemented by Visa or the Member

The updates shall be deemed part of the Visa products or services and subject to the applicable terms and conditions under the Visa Rules.

ID# 0029560   **Edition: Apr 2020 | Last Updated: Apr 2020**

1.1.1.9   Restriction on Use of Visa Materials

Unless otherwise expressly permitted in the Visa Rules, a Member must not, and must not permit or enable others to, do any of the following:

- Use or make copies, in whole or in part, of any aspect of any software, software development kits, APIs, documentation, tools, or other materials provided to the Member in connection with a Visa product, service, and/or program
- Disclose or distribute any Visa materials or any implementations thereof
- Reverse engineer, decompile, disassemble, or otherwise attempt to obtain the underlying ideas, algorithms, structure, or organization of any Visa product or service, or any component thereof, except to the extent that any of the foregoing are not permitted to be restricted under applicable law
- Attempt to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection or security mechanisms in any Visa product or service, or any related component
- Alter or remove any copyright, trademark, trade name, patent, or other proprietary rights notice, legend, symbol, or the like appearing on or in any Visa materials

ID# 0030681   **Edition: Apr 2020 | Last Updated: New**

1.1.1.10   Countries and Territories in Visa Regions

The Visa Regions are comprised of the countries and/or territories listed below.

Table 1-1: Asia-Pacific Region

American Samoa; Australia (including Cocos [Keeling] Islands, Heard Island and McDonald Islands, Norfolk Island, Lord Howe Island, Macquarie Island); Bangladesh; Bhutan; British Indian Ocean Territory; Brunei; Cambodia; Mainland China; Cook Islands; Crozet Islands; Democratic People's Republic of Korea; Fiji (including Rotuma Island); French Polynesia; Guam; Hong Kong; India; Indonesia; Japan; Kerguelen Island; Kiribati (including Canton and Enderbury Islands, Christmas Island (Kiritimati), Fanning Island, Malden Island, Starbuck Island, Washington Island); Laos; Macau; Malaysia; Maldives; Marshall Islands; Mascarene

Visa Core Rules

Visa Core Rules and Visa Product and Service Rules

Table 1-1: Asia-Pacific Region (continued)

Islands; Micronesia; Mongolia; Myanmar; Nauru; Nepal; New Caledonia; New Zealand (including Antipodes Island, Auckland Island, Bounty Island, Campbell Island, Chatham Island, Kermadec Island, Stewart Island); Niue; Northern Mariana Islands; Palau; Papua New Guinea; Pescadores Island; Philippines; Pitcairn Islands; Republic of Korea; Rodrigues Island; Samoa; Singapore; Solomon Islands; Sri Lanka; St. Paul Island; Taiwan; Thailand; Timor-Leste; Tokelau; Tonga; Tuvalu; US Minor Outlying Islands (including Baker Island, Howland Island, Jarvis Island, Johnston Island, Midway Island, Palmyra Island, Wake Island); Vanuatu; Vietnam; Wallis and Futuna

Table 1-2: Canada Region

Canada

Table 1-3: Central and Eastern Europe, Middle East and Africa Region

Afghanistan; Albania; Algeria; Angola; Armenia; Azerbaijan; Bahrain; Belarus; Benin; Bosnia and Herzegovina; Botswana; Bouvet Island; Burkina Faso; Burundi; Cameroon; Cape Verde; Central African Republic; Chad; Comoros; Congo (Brazzaville); Côte d'Ivoire (Ivory Coast); Democratic Republic of the Congo; Djibouti; Egypt; Equatorial Guinea; Eritrea; Eswatini; Ethiopia; Gabon; Gambia; Georgia; Ghana; Guinea; Guinea-Bissau; Iran; Iraq; Jordan; Kazakhstan; Kenya; Kosovo; Kuwait; Kyrgyzstan; Lebanon; Lesotho; Liberia; Libya; Madagascar; Malawi; Mali; Mauritania; Mauritius; Moldova; Montenegro; Morocco; Mozambique; Namibia; Niger; Nigeria; North Macedonia; Oman; Pakistan; Qatar; Reunion; Russian Federation (including Franz Josef Land, Komandorskiye Island, New Siberian Island, Novaya Zemlya, Ostrov Ratmanova, Sakhalin, Severnaya Zemlya); Rwanda; Saint Helena, Ascension, and Tristan da Cunha (including Gough Island); Sao Tome and Principe; Saudi Arabia; Senegal; Serbia; Seychelles; Sierra Leone; Somalia; South Africa; South Sudan; Sudan; Syria; Tajikistan; Tanzania; Togo; Tunisia; Turkmenistan; Uganda; Ukraine; United Arab Emirates; Uzbekistan; Western Sahara; Yemen; Zambia; Zimbabwe

Table 1-4: Europe Region

Andorra; Austria; Bear Island; Belgium; Bulgaria; Channel Islands; Croatia; Cyprus; Czech Republic; Denmark; Estonia; Faroe Islands; Finland (including Aland Islands); France (including its "DOM-TOMs"); Germany; Gibraltar; Greece; Greenland; Hungary; Iceland; Republic of Ireland; Isle of Man; Israel; Italy; Latvia; Liechtenstein; Lithuania; Luxembourg; Malta; Monaco; Netherlands; Norway; Poland; Portugal (including Azores, Madeira); Romania; San Marino; Slovakia; Slovenia; Spain (including Canary Islands, Ceuta, Melilla); Sweden; Switzerland; Turkey; United Kingdom; Vatican City

Visa Core Rules

1 Visa Core Rules

Visa Core Rules and Visa Product and Service Rules

Table 1-5: Latin America and Caribbean Region

Anguilla; Antigua and Barbuda; Argentina; Aruba; Bahamas; Barbados; Belize; Bermuda; Bolivia; Bonaire, Sint Eustatius, and Saba; Brazil; British Virgin Islands; Cayman Islands; Chile; Colombia; Costa Rica; Cuba; Curacao; Dominica; Dominican Republic; Ecuador; El Salvador; Grenada; Guadeloupe; Guatemala; Guyana; Haiti; Honduras; Jamaica; Martinique; Mexico; Montserrat; Nicaragua; Panama; Paraguay; Peru; Puerto Rico; Saint Kitts and Nevis; Saint Vincent and the Grenadines; Sint Maarten; St. Lucia; Suriname; Trinidad and Tobago; Turks and Caicos Islands; US Virgin Islands; Uruguay; Venezuela

Table 1-6: US Region

United States of America

ID# 0027823	Edition: Apr 2020	Last Updated: Apr 2019

1.1.1.12   Visa Canada Member Responsibilities – Canada Region

In the Canada Region: A Member must perform obligations imposed on Visa Canada under the Visa Rules that arise out of Interchange or a Transaction resulting in Interchange between the Member and a non-Member of Visa Canada.

A Member must not do anything to cause Visa Canada to violate the Visa Rules.

ID# 0003768	Edition: Apr 2020	Last Updated: Oct 2014

1.1.1.13   Obligation to Comply with the Code of Conduct – Canada Region

In the Canada Region: All Members must abide by the *Code of Conduct for the Credit and Debit Card Industry* as it may be amended from time to time and adopted by Visa (the "Code").

Each Member acknowledges and agrees that Visa may interpret the Code in accordance with any published interpretation bulletins or guidance issued by the Financial Consumer Agency of Canada.

Members must ensure that all participants for which the Member is responsible under the Visa Rules, including participants that interact directly or indirectly with Merchants or Cardholders (including without limitation, VisaNet Processors and Third Party Agents) on behalf of the Member must abide by the Code.

Effective through 31 January 2020 All Members are required, on an annual basis, to submit to Visa:

- By 31 January of each year, an officer's certificate, in the form attached as (Schedule A-1), confirming its compliance with the Code

- By 15 August of each year, a *Code of Conduct Compliance Questionnaire* in the form required by Visa

A Member that fails to submit a completed officer's certificate or questionnaire as required will be subject to a non-compliance assessment of CAD 100,000 per month of non-compliance.

Effective 1 February 2020 All Members are required, on an annual basis, to submit to Visa by 31 January of each year, an officer's *Attestation of Compliance*, confirming its compliance with the Code.

Visa may require periodic reviews to oversee and monitor compliance with the Code of Conduct and will provide Members with a minimum of 30 calendar days' notice of such reviews.

A Member that fails to submit a completed officer's *Attestation of Compliance* or to provide Visa with information required due to the review will be subject to a non-compliance assessment of CAD 100,000 per month of non-compliance.

Visa may, in its sole discretion, charge any Member or Members fees charged to Visa Canada by the Financial Consumer Agency of Canada with respect to compliance with the Code, where such fee is attributable to that Member or its VisaNet Processor or its Third Party Agent.

ID# 0025973	Edition: Apr 2020	Last Updated: Apr 2020

1.1.1.15   Visa U.S.A., Inc. Member Responsibilities – US Region

In the US Region: A Member must perform all obligations imposed on Visa U.S.A. Inc. under the Visa Rules that arise out of Interchange or a Transaction resulting in Interchange between the Member and a non-Member of Visa U.S.A. Inc.

The Member must not do anything to cause Visa U.S.A. Inc. to violate the Visa Rules. An Acquirer is responsible for Visa Transactions it submits into Interchange regardless of the Acquirer's ability to return the Transaction to the Merchant for any reason.

ID# 0000349	Edition: Apr 2020	Last Updated: Oct 2017

1.1.1.16   Obligation to Comply with Code of Conduct – Europe Region (Germany)

In the Europe Region (Germany): A Member must comply with the Code of Conduct (Verhaltenscodex).

An Acquirer must provide to its Merchants documentation outlining the relationship between the Acquirer and the Merchant, which does not replace the written contract between the Acquirer and Merchant.

An Acquirer must submit annually to Visa the following data:

- Number of newly acquired Merchants
- Number of closed Merchant accounts

ID# 0030042	Edition: Apr 2020 | Last Updated: Oct 2017

1.1.2   Local, Domestic, and Regional Rules and Private Agreements

1.1.2.3   Transaction Country Rules

Regardless of how an Authorization or Transaction is routed or where it is processed, a Transaction is subject to the applicable Visa Rules affecting the Transaction Country. These rules may be superseded by either Private Agreements or the operating regulations of Group Members.

Private Agreements must exclude Interchange originating from an Airline that participates in the International Airline Program.

ID# 0008844	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.3   Waivers

1.1.3.1   Waivers to the Visa Rules

A Member that cannot comply with a rule or requirement in the Visa Rules must submit a Waiver request to Visa.

If the Member cannot comply due to applicable laws or regulations that contravene the Visa Rules, Visa may require proof of the specific laws or regulations, in English or accompanied by a certified English translation.

Visa will notify the Member in writing of its decision on a Waiver request. The Waiver is effective as specified in such Notification.

Each Waiver granted by Visa is unique, may include specific conditions, and is limited only to the specific circumstances of the individual request. A Member must not apply a previously granted Waiver to any other future programs or services or consider a previously granted Waiver as determining the outcome of future requests.

Visa may repeal, amend, extend, or revoke any Waiver upon Notification to the Member.

Visa Core Rules

1 Visa Core Rules

Visa Core Rules and Visa Product and Service Rules

ID# 0025926	Edition: Apr 2020 | Last Updated: Oct 2016

1.1.4   Operating Certificates

1.1.4.1   Operating Certificate Filing

A Member or Non-Member Administrator must submit a complete and accurate Operating Certificate and include Interchange Transactions, On-Us Transactions, and other Transactions that are not processed through VisaNet, as specified by Visa.

The Operating Certificate must be executed by an authorized officer of the Member or Non-Member Administrator.

The Member or Non-Member Administrator must maintain records that allow for an accurate determination and verification of the information contained in each Operating Certificate and provide the records upon Visa request.

ID# 0027829	Edition: Apr 2020 | Last Updated: Apr 2016

1.1.4.2   Exchange Rates for Operating Certificates

A Member (or its Sponsor) must use the exchange rate provided by Visa to file an Operating Certificate when a conversion is required. The quarterly exchange rate is provided via Operating Certificate tools and is a simple average of 3 monthly spot rates for the quarter, sourced from the Financial Times and Thomson Reuters.

ID# 0008837	Edition: Apr 2020 | Last Updated: Oct 2017

1.1.5   Confidentiality

1.1.5.1   Visa Confidential and Visa Restricted Materials – Member Responsibilities

A Member must comply, and must ensure that its Merchants and agents comply, with all of the following:

- Maintain Visa Confidential and Visa Restricted information in strict confidence
- Not disclose any Visa Confidential or Visa Restricted information, unless expressly permitted or required by Visa
- Store and handle Visa Confidential and Visa Restricted information in such a way as to prevent unauthorized disclosure

- Take reasonable measures to protect Visa Confidential and Visa Restricted information and treat it with at least the degree of care with which a Member treats its own confidential and proprietary information, or in case of Visa Restricted information, as follows:
  - For information labeled or otherwise designated as Visa Restricted, in accordance with Visa handling instructions, which may be delivered with its transmission or in its content
  - For information labeled or otherwise designated as Visa Restricted – Personal Data, with the strongest level of protection (including encryption or sufficient compensating controls, and limited distribution for any transmissions) applied by the Member for its highly sensitive information

- Disclose Visa Confidential or Visa Restricted information only to those employees with specific need to know

- Immediately upon Visa request, return to Visa, or destroy, originals and all copies of any Visa Confidential or Visa Restricted information in any medium and, if required by Visa, certify that it has done so

- Notify Visa immediately in the event that the Member becomes legally compelled to disclose any Visa Confidential or Visa Restricted information and, if legally required to disclose any Visa Confidential or Visa Restricted information, only disclose that portion that it is legally required to disclose

- Process and transfer personal data (whether or not it is classified as Visa Confidential or Visa Restricted information) in accordance with the Visa Rules and applicable laws or regulations

ID# 0000467	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.5.2   Confidentiality of VisaNet Information

Information regarding VisaNet is proprietary and Visa Confidential. A Member and its Merchants and agents must take appropriate action, by agreement or otherwise, to ensure that its employees or agents with access to VisaNet are all of the following:

- Advised of the confidential and proprietary nature of these systems

- Prohibited from providing access to or disclosing these systems to any third party

- Prohibited from using these systems for any purpose not authorized in the Visa Rules

ID# 0003669	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.5.3   Use or Disclosure of Confidential Information

A Member must not publish, disclose, convey, or distribute to any person or organization, or use for filing patents, any Visa confidential or proprietary information (including, but not limited to,

documents, ideas, products, and data) without the prior written approval of Visa.

This does not apply to:

- A third party (organization, or person, including contractors), if both of the following apply:
  - The third party is providing services to the Member and the disclosure is required to perform services in connection to the Member's Visa Program
  - The third party does not compete with Visa with respect to Visa or its Members with respect to their Visa Programs
- The Member's parents or subsidiaries that do not participate in a competing payment program
- Information that has been publicly released by Visa

A Member that discloses information to a third party must have a written agreement with the third party that it:

- Will not disclose the confidential information to any other third party
- Will use the confidential information only to provide services to the Member for use only with the Member's Visa products and services

Any confidential information disclosed to the third party must comply with all of the following:

- Remain solely the property of Visa
- Be returned to Visa immediately upon Visa request
- Be returned to the Member immediately upon termination of the relationship that required use of the confidential information

The Member is responsible for the third party's compliance with these conditions and must not allow a non-Member VisaNet Processor to use the V.I.P. System or BASE II unless the non-Member VisaNet Processor has delivered to Visa a completed *VisaNet Letter of Agreement (Exhibit 5A)*.

Unauthorized use or disclosure of Visa Confidential information by a Member in connection with any patents or patent applications grants to Visa a fully paid-up, royalty-free, worldwide, irrevocable license to exercise all rights under that patent, including the right to grant and authorize sublicenses.

ID# 0006467	Edition: Apr 2020	Last Updated: Apr 2017

1.1.5.4   Confidentiality of Visa Systems Information

A Member, VisaNet Processor acting on behalf of a Member, Merchant or its agent, or Visa Direct Connect Merchant[1] must take appropriate action to ensure that its employees or agents with access to VisaNet or related documentation comply with all of the following:

- Are advised of the confidential and proprietary nature of these systems and documentation

- Use their best efforts to protect the VisaNet Access Points

- Are prohibited from both:

  – Providing access to or disclosing these systems and documentation to any third party

  – Using these systems and documentation for any purpose not authorized in the Visa Rules

A Member, Merchant or its agent, or Visa Direct Connect Merchant[1] must not disclose any confidential information of Visa or its subsidiaries to a non-Member.

[1] In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region*, it must refer to *Visa Europe Operating Regulations – Processing.*

ID# 0027073	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.5.5   Visa Disclosure of Confidential Member Information

Visa and its subsidiaries will not disclose to any third party any confidential, proprietary matters of any Member including, but not limited to, documents, ideas, products, and data, other than for any of the following:

- Disclosure in the ordinary course of business to provide services to a Member or a Member's designated Agent, including, but not limited to, all of the following:

  – Completing a Transaction

  – Risk control

  – Dispute resolution

  – Marketing services

- Disclosure with the consent of the Member

- Disclosure of data that is aggregated so as not to disclose the data of any single Member

- Other disclosure that is in accordance with applicable laws or regulations

ID# 0029983	Edition: Apr 2020 | Last Updated: Apr 2017

1.1.5.6   Visa Use and Disclosure of Confidential Consumer Cardholder Information – US Region

In the US Region: Visa and its subsidiaries will not use or disclose Confidential Consumer Cardholder Information to third parties, other than for any of the following:

- Use or disclosure in the ordinary course of business to provide services to a Member or a Member's designated Agent, including, but not limited to, all of the following:
  - Completing a Transaction
  - Risk control
  - Dispute resolution
  - Marketing services
- Use or disclosure with the consent of the Cardholder
- Other use or disclosure that is in accordance with applicable laws or regulations

ID# 0000508	Edition: Apr 2020 | Last Updated: Oct 2014

1.1.6   Visa Rights

1.1.6.1   Visa Ownership of Intellectual Property

A participant in the Visa system must recognize Visa's ownership of its intellectual property, including the Visa name, Visa Marks, and Visa technology, and agree to protect these ownership rights and the integrity of the Marks by complying with the applicable Visa Rules in all activities, including issuing, acquiring, and processing.

A Member or Visa Direct Connect Merchant[1] does not have any property or other right, claim, or interest, including any patent right, trade secret right, or copyright interest, in VisaNet, or in any systems, processes, equipment, software, data, or materials that Visa or its subsidiaries use with VisaNet, or in connection with a Visa Program, except for Merchant- or Member-supplied data or equipment.

[1]   In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2 Applicability of Processing Rules – Europe Region*, it must refer to *Visa Europe Operating Regulations – Processing*.

ID# 0007727	Edition: Apr 2020 | Last Updated: Apr 2018

1.1.6.2   Visa Right to Monitor, Audit, Inspect, and Investigate

At its sole discretion, at any time, Visa may, either itself or through an agent, do any of the following:

- Investigate, review, audit, or inspect a Member, or the Member's agents, Merchants, Marketplaces, Sponsored Merchants, Payment Facilitators, or Digital Wallet Operators, including by inspecting the premises and auditing the books, records, and procedures of the Member, agent, Merchant, Marketplace, Sponsored Merchant, Payment Facilitator, or Digital Wallet

Operator to ensure that it is complying with the Visa Charter Documents, Visa Rules, and applicable brand and security standards and procedures, and operating in a safe and sound manner

- Monitor, investigate, review, audit, or inspect the premises, books, records, or procedures of a Visa-approved vendor or Third-Party Personalizer, including security and quality control procedures of each Visa-approved manufacturer and Third-Party Personalizer

- Obtain from any Visa-approved manufacturer or Third-Party Personalizer a production-run sample of a Card that includes all security features

- In addition, in the Europe Region:

  – Require a Visa Commercial Card Issuer to impose an obligation on its agents and any other entities that participate in the Issuer's multinational programs to permit Visa to audit those agents and other entities

  – Require a Merchant Agreement with a Merchant that sells Prepaid Cards to allow Visa to audit the records and procedures of the Merchant

A Member must cooperate fully, and ensure that its agent, Merchant, Marketplace, Sponsored Merchant, Payment Facilitator, or Digital Wallet Operator cooperates fully, with Visa in any such investigation, inspection, audit, or review. This cooperation includes providing access to the premises and to all pertinent records, including financial reports, and releasing any information to Visa upon request within the stipulated timeframe.

Any investigation, inspection, review, or audit will be conducted at the Member's expense, unless otherwise specified in the applicable Fee Schedule.

ID# 0007121	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.6.3   Right to Impose Conditions on Visa Product or Visa Service Participation

Participation in or use of a Visa service or Visa product is at the discretion of Visa, which may limit or impose conditions on its use, and may discontinue the service or product at any time.

ID# 0028039	Edition: Apr 2020 | Last Updated: Oct 2014

1.1.6.4   Right to Use Patents Relating to Visa Tokenization Services

In partial consideration for participation in or use of Visa tokenization services, a Member grants Visa a fully paid-up, royalty-free, worldwide, non-exclusive, irrevocable, non-terminable license and covenant not to sue (and not to assist or provide consent to sue) under patents to make, have made, use, offer for sale, sell, import, and otherwise provide Visa tokenization services (or any portion thereof) and to practice any method, process, or procedure in connection therewith. The Member grants and extends the foregoing license and covenant not to sue to Visa tokenization

service participants, users, business partners, contractors, agents, processors, and service providers and hereby irrevocably covenants not to rely upon or refer to the Visa tokenization service or any portion, functionality, or other characteristics thereof in any assertion or allegation of patent infringement (direct or indirect) or to assist or provide consent to do so.

ID# 0029513	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.6.5   Right to Use Member Feedback

Visa has, and a Member grants, the right to use, disclose, distribute, or commercialize generally for itself and others any feedback, ideas, suggestions, submissions, data, or information (whether provided in written or oral form), and all intellectual property rights relating thereto, that Visa, its subsidiaries, or its affiliates receive from a Member in connection with Visa products, programs, services, or systems for any and all purposes.

ID# 0029514	Edition: Apr 2020 | Last Updated: Apr 2017

1.1.6.6   Investigation Response Requirement

A Member must respond to and provide information requested by Visa for a Visa Rules violation that is under investigation.

The Member must submit its response and information, within the time period specified, by mail, courier, facsimile, hand, email, or other electronic delivery method. The Notification response is effective when posted, sent, or transmitted by the Member or its agent to Visa.

ID# 0025974	Edition: Apr 2020 | Last Updated: Oct 2014

1.1.6.7   Right to Request Cards

Visa may request a functional Card or Proprietary Card or access to any New Channel associated with a BIN licensed or used by an Issuer.

Upon written request, an Issuer must both:

- Provide Visa with a Card or a Proprietary Card or access to any New Channel and its associated PIN within 30 calendar days
- Personalize the Card or Proprietary Card or New Channel, as specified by Visa

ID# 0026009	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.7   Use of VisaNet

1.1.7.1   Non-Assignable Right to Use VisaNet

A Member's, VisaNet Processor's, or Visa Direct Connect Merchant's[1] right to use VisaNet is not assignable and its duties are non-delegable without prior written consent from Visa. However, a Member or Visa Direct Connect Merchant[1] may use a non-Member VisaNet Processor that has executed and delivered to Visa a *VisaNet Letter of Agreement* (Exhibit 5A).

A VisaNet Processor or Visa Direct Connect Merchant[1] acknowledges and agrees that the VisaNet endpoint connectivity is a Visa asset and not transferable without the express written consent of Visa. A VisaNet Processor or Visa Direct Connect Merchant must not transfer its VisaNet endpoint to another Member or Agent. It must notify Visa in writing at least 90 days before the effective date of a change, for example, but not limited to, a sale of all or substantially all of the assets of the operation, acquisition, merger, ownership change, or financial restructuring, and promptly provide Visa with any related information that is requested.

[1] In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region*, it must refer to *Visa Europe Operating Regulations – Processing*.

ID# 0003081	Edition: Apr 2020	Last Updated: Oct 2019

1.1.8   Liabilities and Indemnifications

1.1.8.1   Taking Responsibility

Each Member is solely responsible for its issuance of Visa products and acquiring of Merchants to accept Visa products, including responsibility for settlement of Transactions, compliance with the Visa Charter Documents and the *Visa Core Rules and Visa Product and Service Rules*, and ensuring that their Visa programs comply with all applicable legal and regulatory requirements. Each Member shall Indemnify Visa for and against Claims and Liabilities arising out of or in connection with its issuance of Visa products and acquiring of Merchants, and broadly disclaims liability against Visa for such activities.

ID# 0007758	Edition: Apr 2020	Last Updated: Apr 2018

1.1.8.2   Member Participation in Visa Network

Effective 18 April 2020 A Member understands that Visa provides a network and desires to provide programs, products, and services to enable partners, end users, and other participants to benefit widely from the network. In exchange for participation in and benefits resulting from such programs, products, and services, a Member agrees not to (and not to authorize, assist, or encourage others to) assert against Visa, its affiliates, their contractors, agents, and service providers

working on their behalf to provide such Visa programs, products, and services, or other participants, any patent infringement claim involving any activity regarding the program, products, services, and associated materials provided by Visa.

ID# 0030682	Edition: Apr 2020	Last Updated: New

1.1.8.24   Responsibility for Losses Caused by VisaNet Processors

A Member is responsible for any and all losses caused by its VisaNet Processor. All Members using a Clearing or authorizing VisaNet Processor, whether a Member or non-Member, are jointly and severally responsible for the proper performance by that VisaNet Processor of all the requirements of the Visa Rules.

ID# 0025873	Edition: Apr 2020	Last Updated: Oct 2014

1.1.8.25   Limitation of Liability for VisaNet Processors

A Member may limit its liability for the failure of a VisaNet Processor if it provides Visa with an updated *VisaNet Processor and Third Party Registration and Designation (Exhibit 5E)* showing that it had terminated the VisaNet Processor relationship before the failure.

This limitation of liability is effective upon receipt by Visa of Member notification.

ID# 0025887	Edition: Apr 2020	Last Updated: Oct 2014

1.1.8.30   Member Responsibility for Agents – Europe Region

In the Europe Region: A Member must include in its agreements with its respective agents a term that provides that the Member is responsible for the acts or omissions of the agents.

ID# 0029767	Edition: Apr 2020	Last Updated: Oct 2016

1.1.8.54   ATM Member Liability for Plus Shared Deposit Service

An Issuer participating in the Shared Deposit Service is responsible to the Acquirer for any and all Claims and Liabilities (including returned checks, Dispute Responses, forged or altered checks) or expenses (for example: processing ineligible deposit items) that are incurred and arise out of or are in connection with the processing of the Shared Deposit Transaction.

The maximum damage for an Acquirer's failure to comply with the requirements specified in *Section 6.3.3.2, Acquirer Participation in the Plus Shared Deposit Service,* and *Section 6.3.3.3, Shared Deposit Service – Acquirer Responsibilities,* with respect to a particular deposit is limited to the amount incurred by the Issuer with respect to that deposit, not to exceed the amount of the

deposit, reduced by the amount of loss that the Issuer would have incurred even if the Acquirer had complied with the applicable rules. In addition, the Acquirer will not be liable to the Issuer for any amount that the Issuer could have recovered from its Cardholder.

ID# 0030594	Edition: Apr 2020 | Last Updated: Apr 2019

1.1.8.56   Visa Central Travel Account – Issuer Liability

An Issuer assumes full liability for any misuse on physical Cards issued on a Visa Central Travel Account.

ID# 0026397	Edition: Apr 2020 | Last Updated: Oct 2019

1.1.8.57   Liability for Misencoded Cards

Visa assigns liability for payment of Transaction Receipts resulting from the use of a misencoded Card as follows:

- To the Acquirer that received the Transaction Receipt, if the misencoded Card bears a BIN that was not assigned to an Issuer. The Acquirer is liable until both:
  - The misencoded Card is recovered.
  - Visa identifies the Issuer that ordered its manufacture.
- To the Issuer to which the BIN is assigned, if an Acquirer receives a misencoded Card bearing a valid BIN but an invalid Account Number. The Issuer is liable both:
  - If the Acquirer presents the Transaction Receipt within 180 calendar days of the Transaction Date
  - Until the Issuer that ordered the manufacture of the Card is identified

In the Europe Region: There is no time limit on a Member's right to reassign liability to the Issuer.

ID# 0001813	Edition: Apr 2020 | Last Updated: Apr 2020

1.1.8.58   Liability for Misembossed or Misencoded Cards – US Region

In the US Region: Visa assigns liability for payment of Transaction Receipts resulting from the use of misembossed or misencoded Cards based on the following priorities in the order shown:

- Issuer that appears on the misembossed or misencoded Card, if the Card has been recovered
- Issuer whose BIN appears on the Transaction Receipt, if the misembossed or misencoded Card has not been recovered or if the name of the Issuer does not appear on the Card

- Issuer that first received the Transaction Receipt. If the misembossed or misencoded Card is recovered within 12 months of the Transaction Date, the Issuer may transfer liability for the Transaction Receipt to the Issuer that appears on the misembossed or misencoded Card.

ID# 0001817	Edition: Apr 2020 | Last Updated: Oct 2019

1.2   Licensing and Numerics Management

1.2.1   Licensing – General Membership

1.2.1.1   BIN and Acquiring Identifier Use and Jurisdiction

A BIN Licensee or an Acquiring Identifier Licensee or a BIN Licensee's or Acquiring Identifier Licensee's Sponsored Member must use a BIN or an Acquiring Identifier only:

- For programs and activity as agreed and licensed by Visa

- As specified by Visa requirements and procedures for licensing and use

- In a country in which the BIN Licensee or Acquiring Identifier Licensee is licensed

A BIN or an Acquiring Identifier is licensed for use in a single country, except as specified for the following:

- Visa Multinational Program

- Visa Prepaid program

- International Airline Program

- In the Europe Region: A Member that has passported its license to a Host Country in line with EU passporting legislation

Visa will recover a BIN or an Acquiring Identifier that remains uninstalled in Visa systems for 12 months after its assignment.

ID# 0001250	Edition: Apr 2020 | Last Updated: Apr 2020

1.2.1.4   Prohibition of BIN or Acquiring Identifier Sale or Exchange

A BIN Licensee or an Acquiring Identifier Licensee must not sell, rent, or exchange any BIN or Acquiring Identifier. In the event of a portfolio sale or merger, the BIN Licensee or Acquiring Identifier Licensee is responsible for notifying Visa.

ID# 0001238	Edition: Apr 2020 | Last Updated: Oct 2019

1.3   Use of Marks

1.3.1   Marks License

1.3.1.1   Visa Proprietary Rights to the Visa-Owned Marks and Visa Brand Name

Members acknowledge the proprietary rights of Visa and that unauthorized or inappropriate use of the Visa-Owned Marks and Visa Brand Name may cause Visa irreparable damage or injury. Visa has the full authority to enforce all Visa rules governing Members, Merchants, agents, and other entities that use the Visa-Owned Marks and Visa Brand Name.

ID# 0007432	Edition: Apr 2020	Last Updated: Oct 2014

1.3.1.2   Infringement Proceedings Regarding the Visa-Owned Marks

Unless Visa grants express consent, Visa reserves the sole right to initiate infringement proceedings or other challenges involving any use of the Visa-Owned Marks.

ID# 0006462	Edition: Apr 2020	Last Updated: Oct 2014

1.3.1.3   Denotation Requirements for Visa-Owned Marks

A Member must not use any denotation or legend of Marks registration or ownership in connection with the Visa-Owned Marks, except as required or approved by Visa. Upon the Member's written request, Visa will both:

- Advise whether a denotation or legend must be used in a specific country
- Provide the appropriate denotation or legend to be used with Visa-Owned Marks

ID# 0006464	Edition: Apr 2020	Last Updated: Apr 2017

1.3.2   General Use of Marks

1.3.2.1   Visa Program Marks List

The Visa Program Marks include:

- Visa Flag Symbol
- Visa Brand Mark
- Visa Brand Name

- Visa wordmark
- Dove design
- Any other Mark that Visa adopts for use with the Visa Program

ID# 0006267	Edition: Apr 2020 | Last Updated: Oct 2015

1.3.2.2   Use and Protection of the Visa-Owned Marks

The Visa-Owned Marks must appear exactly as shown in the _Visa Product Brand Standards._

A Member must cooperate with Visa to ensure protection of each of the Visa-Owned Marks and must ensure that all use of the Visa-Owned Marks, as well as the nature and quality of all services rendered under these Marks, complies with the Visa Rules.

If requested, a Member must supply Visa with samples of any materials produced by or for the Member that bear a Visa-Owned Mark.

ID# 0003581	Edition: Apr 2020 | Last Updated: Oct 2016

1.3.2.3   Card Design Requirements

All Card designs must comply with the _Visa Product Brand Standards._

ID# 0006160	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.2.4   Restricted Use of the Visa-Owned Marks

A Member must use the Visa-Owned Marks, including associated elements, only for the following:

- To denote or promote a Visa Program or Visa products, offers, sponsorships, services, processing, or acceptance
- To promote a Member's Visa Program

ID# 0006308	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.2.5   Member Use of Country Name with the Visa-Owned Marks

A Member must not use the name of a country with the Visa Brand Name or any other Visa-Owned Mark in its corporate name or other business name, unless Visa has granted exclusive jurisdiction to the Member under the _Visa International Certificate of Incorporation and By-Laws_ and has granted express permission.

A country name may be used in a Member's corporate name in which the country name is an integral part.

| ID# 0007643 | Edition: Apr 2020 | Last Updated: Oct 2016 |

1.3.2.6   Use of "Visa" in Group Member Corporate Identity

In a country with a single Group Member, the Group Member may use "Visa" as a part of its corporate legal name and identity, as permitted in the Visa Rules.

In a country with multiple Group Members, a Group Member must not use "Visa" (including the Visa-owned Marks) as part of its corporate legal name or identity. When multiple Group Members exist in the same country, 12 months after the formation of a new Group Member, an existing Group Member must not use the name "Visa" in its corporate name and identity.

| ID# 0006274 | Edition: Apr 2020 | Last Updated: Oct 2016 |

1.3.2.7   National Organization Use of Visa Name

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A National Organization established in compliance with Article XVI of the *Visa International Certificate of Incorporation and By-Laws* may use "Visa" as part of its corporate legal name and identity, as provided in the Visa Rules.

In the Europe Region: A National Organization established in compliance with the *Visa Europe Limited Membership Regulations* must not use "Visa" or any of the Visa-Owned Marks as part of its corporate legal name and identity, unless Visa had granted consent to do so before 1 October 2007.

| ID# 0006276 | Edition: Apr 2020 | Last Updated: Oct 2016 |

1.3.2.8   "Visa" as Part of Corporate Identity

A Member must obtain written approval from Visa to use the name "Visa" or any other Visa-Owned Mark as part of its corporate name or identity. If permission is granted, the name or Mark must be used:

- In the Member's corporate name, with the country identifier. The name "Visa" must not be used without the country identifier.
- In all media (for example, business cards, letterhead, press releases, websites), with a clear indication of actual corporate identity, including full legal name

- In a contract or legal instrument with third parties. The Member must clearly state that it does not have the authority to act (and is not acting) as an agent of, or represent, Visa or any affiliate of Visa.

- Solely for the promotion of Visa products and services

ID# 0007277	Edition: Apr 2020 | Last Updated: Oct 2016

1.3.2.9   Ownership of Visa-Owned Marks

A Member must not state or imply that it is the exclusive owner or provider of any Visa-Owned Mark, Visa Card Product, or Visa Program, except as otherwise permitted in the Visa Rules.

ID# 0006503	Edition: Apr 2020 | Last Updated: Oct 2016

1.3.2.10   Visa Endorsement of Goods/Services

A Member must not use any of the Visa-Owned Marks to indicate that Visa endorses, is identified with, or sponsors goods or services other than those of Visa.

ID# 0006555	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.2.12   Use of Visa-Owned Marks in Marketing Materials

In marketing collateral, a Member must not use:

- A Visa-Owned Mark in such a way that it could be mistaken for an actual Card and used in a Transaction

- The Visa Brand Name in any classified advertising section, except to indicate the availability of Visa Program services and other Card services

- The Visa Brand Name on a check

ID# 0008273	Edition: Apr 2020 | Last Updated: Oct 2016

1.3.2.13   Card Reproduction Prohibition

A Member must not distribute or display a reproduction of a Card as an indication of acceptance of Visa products at the Point-of-Transaction.

Only the Visa Brand Mark may be used to denote acceptance at the point of sale.

ID# 0006329	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.2.14   Obscured/Defaced Visa-Owned Marks

No portion of a Visa-Owned Mark may be obscured, distorted, or defaced.

A Visa-Owned Mark that is a graphic design must not be used separately.

ID# 0003578	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.3   Protecting the Visa Brand

1.3.3.1   Protecting the Visa Brand Reputation

No activities or materials may infringe, dilute, denigrate, or impair the goodwill and/or reputation of the Visa brand or Visa-Owned Marks.

ID# 0007762	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.3.2   Prohibition of Marks Infringement and Brand Denigration

A Member's Visa Card Program, Visa Electron Program, Visa Secure, or Visa TravelMoney Program materials, including Global Co-branded Card and Affinity/Co-Branded Card materials or other Member materials using any Mark(s) of the Visa Card Program, must not contain any matter that would tend to infringe, dilute, degrade, or denigrate any of the Visa-Owned Marks, Visa products, Visa services, or any Member or Merchant or impair the reputation or goodwill of Visa or the goodwill associated with the Marks.

An Issuer that engages in Dual Payment Card Marketing must ensure that all communications and marketing material relating to Marks, products, or services of a non-Visa general purpose payment card network, as designated by Visa, are not positioned in conjunction with Visa-Owned Marks, products, or services in a manner that dilutes or denigrates the Visa brand.

ID# 0025557	Edition: Apr 2020 | Last Updated: Apr 2019

1.3.3.3   Marks Use and Marketing Restrictions

A Member must not adopt any Mark, or market, either directly or indirectly, any Visa product or service to consumers, Merchants, or other Members in a manner that has the likely effect of confusing, misleading, defrauding, or deceiving such consumers, Merchants, or Members, either as to the program, product, or service or the source, affiliation, sponsorship, or association of such program, product, or service. Such prohibited acts include, without limitation, making direct or indirect, false, confusing, or misleading statements or failing to disclose a material fact about the programs, products, or services, or any aspect thereof, of a Member, Visa, another Member, a Merchant, or a competitor.

ID# 0025558	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.3.4   Brand Protection and Use of the Visa-Owned Marks

A Member must not use the Visa-Owned Marks:

- In any manner that may bring the Visa-Owned Marks or Visa Inc. or its affiliates into disrepute

- In relation to, or for the purchase or trade of, photographs, video imagery, computer-generated images, cartoons, simulation, or any other media or activities including, but not limited to, any of the following:

  - Child pornography

  - Incest

  - Bestiality

  - Rape (or any other non-consensual sexual behavior)

  - Non-consensual mutilation of a person or body part

A Member that does not comply with these requirements will be subject to non-compliance assessments prescribed under the Global Brand Protection Program.

ID# 0007283	Edition: Apr 2020 | Last Updated: Oct 2016

1.3.4   Marketing, Promotion, and Advertising Materials

1.3.4.1   Visa Review of Brand, Sponsorship, and Marketing Materials

A Member must obtain prior written approval from Visa for all of the following:

- Proposed designs for all form factors intended for use in Visa payments in a physical or digital form.[1,2] These must be submitted to Visa before production and each time the design is changed.

- Use of any Visa-Owned Mark in the Member's sponsorship of any events, including a specific sporting, musical, artistic, or other event.[3] The Member must provide all advertising, promotions, and public relations material for each country in which the sponsorship activity will occur.[4] If a Member plans sponsorship activities in an additional country at a later date, it must submit a new request.

- Dual Payment Card Marketing[5] (including all offers, solicitations, promotions, and communications that include any Visa-Owned Marks or Visa-branded products), before production and distribution

Visa Core Rules and Visa Product and Service Rules

- In the US Region: Use of Limited Acceptance signage for any purpose other than those permitted in the Visa Rules
- In the US Region: All marketing materials or other customer communications pertaining to any of the core and optional services, as specified in the implementation materials available from Visa, before production and distribution

A Member must submit brand or marketing-related materials containing a Visa-Owned Mark for review if requested by Visa.

A Member must use each Visa-Owned Mark within the scope of the written approval from Visa. After Notification from Visa, a Member must correct any improper use of any Visa-Owned Mark.

Visa review or approval of a Card design or brand or marketing-related materials does not:

- Replace the need for a Member to consult with its own legal counsel regarding the use of a Card design or brand or marketing-related materials
- Offer legal protection from possible infringement or other types of actions
- Relieve the Member of its responsibility for accurate disclosure and compliance with legal and regulatory requirements

In the US Region: A Member must not use the Visa-Owned Marks in connection with a Member's promotion, offer, or solicitation of a Visa Card not defined as a US Covered Visa Debit Card, or the maintenance of a US Cardholder relationship for a Visa Card not defined as a US Covered Visa Debit Card, together with Marks that are associated with payment card products issued by the American Express Company, Discover Financial Services, and their subsidiaries or affiliates (including, by way of example and not limitation, "American Express," "Optima," "Discover," "Bravo," "Novus," and "Membership Rewards") or together with Marks associated with any other payment card company deemed competitive by the Board of Directors, if such Marks are owned or controlled by such competitors.

In the US Region or a US Territory: A Member may use the Marks of the American Express Company, MasterCard Worldwide (including Maestro), Discover Financial Services, or the subsidiaries or affiliates of these entities or other entities deemed competitive by Visa in connection with a Member's promotion, offer, or solicitation of a US Covered Visa Debit Card, or the maintenance of a Cardholder relationship for a US Covered Visa Debit Card.

[1] **Effective through 17 April 2020** Visa will retain digital design art and may use it in Visa-sponsored or Visa-owned services in which an Issuer participates. Visa may provide digital design art to a payment Token requestor to display enrolled Cards in a wallet application.
Effective 18 April 2020 Visa in its discretion may retain and use digital design art provided by a Member in connection with the Member's participation in a Visa-sponsored or Visa-owned service. Visa may also provide this digital design art to a payment Token requestor to display enrolled Cards in a digital wallet application or to an Acquirer participating in the Visa Digital Commerce Program (VDCP).

Visa Core Rules and Visa Product and Service Rules

[2] In the Europe Region: An Issuer must submit a completed *Card Design Member Self-Certification Form* for the appropriate product.

[3] Not applicable to the purchase of advertising not specifically tied to the sponsorship of these events.

[4] In the Europe Region: Two months before the anticipated release date of the materials.

[5] In the AP Region: Dual Payment Card Marketing is not allowed for Visa Infinite Business Cards and Visa Ultra High Net Worth Cards.

ID# 0027788	Edition: Apr 2020 | Last Updated: Apr 2020

1.3.4.2   Member Identification

A Member must identify itself by city[1] and principal name, and may substitute a local Branch name and city, if desired, on all supplies, materials (including broadcast), and oral or written solicitations sent to current or prospective Cardholders or Merchants. A Member must not state or imply in these materials that any other Member's Cards or Merchant materials are being replaced, are invalid, or should be destroyed. A Member must not state or imply that Visa provided or endorsed the materials unless Visa designed them for Member use.

[1] In the Europe Region: This does not apply.

ID# 0006311	Edition: Apr 2020 | Last Updated: Oct 2016

1.3.4.3   Merchant Use of the Visa-Owned Marks in Promotions and Advertising

A Member must not allow a Merchant or other entity to use a Visa-Owned Mark for promotional or advertising purposes in any media, unless:

- The Visa Rules permit its use
- The Member distributes the material containing the Visa-Owned Mark
- In the US Region: The Member's name and city appear on the material containing the Visa-Owned Mark, as applicable

ID# 0008277	Edition: Apr 2020 | Last Updated: Oct 2014

1.3.4.4   Use of Competitive Marks with the Visa-Owned Marks

A Member may use certain Visa Program Marks on items other than Cards or for sponsorship activities with the Marks of the following or its subsidiaries or affiliates:

- American Express Company
- Discover Financial Services

- MasterCard Worldwide

- Any other entity Visa deems competitive

The overall appearance of this use must unmistakably convey the idea that the Visa-Owned Mark, when used on items other than Cards or for sponsorship activities, clearly identifies a product or service that is separate and distinct from any product or service of the entities listed above.

In the Europe Region: An Issuer that issues Cards within the European Economic Area may, with the agreement of Visa, use non-Visa-Owned Marks on a Card, including competitive Marks, alongside a Visa-Owned Mark.

In the US Region: A Member must not use the Marks of the American Express Company, MasterCard Worldwide (including Maestro), Discover Financial Services, or the subsidiaries or affiliates of these entities on Cards not defined as US Covered Visa Debit Cards, except that:

- A wordmark may be used to denote ATM sharing only if it appears on the back of a Card, as specified in *Section 3.2.3.3, Use of Other Marks – US Region and US Territories.*

- The PULSE Mark may appear on the back of a Visa Check Card or a Debit Card if the Issuer processes Non-Visa Debit Transactions.

In the US Region: A Member may use the Visa Program Marks in conjunction with the Marks of these entities on items and materials other than Cards provided that the overall appearance resulting from such use unmistakably conveys the idea that the Marks associated with Visa identify a product or service separate and distinct from any product or service of the American Express Company, MasterCard Worldwide (including Maestro), Discover Financial Services, or their subsidiaries or affiliates.

In the US Region or a US Territory: A Member may use the Marks of the American Express Company, MasterCard Worldwide (including Maestro), Discover Financial Services, or the subsidiaries or affiliates of these entities, or other entities deemed competitive by Visa, on US Covered Visa Debit Cards, as specified in the *Visa Product Brand Standards,* provided that the overall appearance resulting from such use unmistakably conveys the idea that the Marks associated with Visa identify a product or service separate and distinct from any product or service of the American Express Company, MasterCard Worldwide (including Maestro), Discover Financial Services, or their subsidiaries or affiliates.

ID# 0006327	Edition: Apr 2020 | Last Updated: Apr 2020

1.3.4.5   Restricted Use of Other Marks

A Member must not use a Mark other than the Visa Brand Mark or Visa Brand Mark with the Electron Identifier on a Card to indicate Card acceptance at a Merchant Outlet outside the country of Card issuance.[1]

A Mark owned by an individual Merchant or a group of Merchants that operate under a common trade name may appear on a Card as part of an Affinity/Co-Brand Program approved by Visa. If this Mark is different than the one used as an identifier of payment services at other Merchant Outlets the Mark is not considered to indicate payment acceptance.

A Member may use non-Visa-owned brand Marks to indicate acceptance at Merchant Outlets solely within the country of Card issuance only if these non-Visa-owned brand Marks are clearly less prominent than the Visa Brand Mark or Visa Brand Mark with the Electron Identifier.[2,3]

Except for the Account Number, a Card must not bear any number or device, whether embossed, printed, etched, encoded, or otherwise affixed, that is used for international payment purposes. This does not apply to a Card issued inside the European Economic Area (EEA) that bears another number, payment application, payment device, or payment scheme to initiate a transaction at a Merchant Outlet inside the EEA. In the Europe Region, an Issuer must notify Visa of its intention to issue such a Card.

A Member must not use the Marks of a non-Visa general purpose payment card network on a Card without prior written consent from Visa.[3]

A Member may use the Visa Program Marks in conjunction with the Marks of these entities on items and materials other than Cards provided that the overall appearance resulting from such use unmistakably conveys the idea that the Marks associated with Visa identify a product or service separate and distinct from any product or service of any non-Visa general purpose payment card network.

[1] In the Europe Region: This does not apply to a Member located in the European Economic Area (EEA), which may use a non-Visa-owned Mark that is as prominent as the Visa Brand Mark to indicate acceptance within the EEA.

[2] In the Canada Region: This does not apply to Cards bearing the Mark of the Interac Association.

[3] In the US Region and US Territories: This does not apply to US Covered Visa Debit Cards.

ID# 0006326   Edition: Apr 2020 | Last Updated: Apr 2020

1.3.4.6   Prohibited Use of Competitive Trade Name or Mark

The following must not appear on any part of a Card:

- Any Trade Name or Mark that identifies or is associated with any entity, or its subsidiaries or affiliates, deemed competitive by Visa,[1,2] including:
  - American Express Company
  - Discover Financial Services[3]
  - MasterCard Worldwide (including Maestro)[4]
- Any Trade Name or Mark that is confusingly similar to any other Visa-Owned Mark

Visa Core Rules

Visa Core Rules and Visa Product and Service Rules

---

¹ In the US Region and US Territories: This does not apply for US Covered Visa Debit Cards.

² In the Europe Region: This does not apply to Cards issued within the European Economic Area.

³ In the US Region: This does not apply for Cards bearing the Pulse Mark and Cards bearing the Plus Symbol.

⁴ In the LAC Region, US Region: This does not apply to certain Cards bearing the Cirrus Wordmark.

ID# 0008458	Edition: Apr 2020 | Last Updated: Apr 2020

1.4   Issuance

1.4.1   Issuance Conditions

1.4.1.1   Offer/Issuance Conditions

A Member must not condition the offer or issuance of any payment card product bearing the Visa Program Marks or the maintenance of a Cardholder relationship upon the possession or acceptance of a product bearing the Marks of the American Express Company, MasterCard Worldwide, Discover Financial Services, Diner's Club, JCB, or any other non-Visa general purpose payment card network, as designated by Visa, without the prior written consent of Visa.

In the US Region or in a US Territory: A Member may condition the offer or issuance of a US Covered Visa Debit Card, or the maintenance of a Cardholder relationship for a US Covered Visa Debit Card, upon the possession or acceptance of a product bearing the Marks of the American Express Company, MasterCard Worldwide, Discover Financial Services, Diner's Club, JCB, or any other non-Visa general purpose payment card network, as specified in the _Visa Product Brand Standards_.

ID# 0025568	Edition: Apr 2020 | Last Updated: Apr 2020

1.4.1.3   New Card Program Third-Party Brand Requirement

A Member must ensure that a new Card program that contains a third-party brand complies with the Affinity/Co-Brand requirements specified in the _Visa Product Brand Standards_.

ID# 0030579	Edition: Apr 2020 | Last Updated: Apr 2020

1.4.1.4   General Member Card Program Requirements – Canada Region

In the Canada Region: A Visa Canada General Member must:

- Operate its own Card program
- Issue Cards in its own legal name or in a Trade Name or Mark owned by the Member and approved by Visa, bearing the Visa-Owned Marks, to eligible Cardholders

ID# 0004091	Edition: Apr 2020	Last Updated: Oct 2014

1.4.2   Account Numbers

1.4.2.1   BINs and Account Numbers on Cards

BIN and Account Number structures embossed, encoded, or printed on a Card

ID# 0003196	Edition: Apr 2020	Last Updated: Apr 2020

1.4.3   Notification and Disclosure

1.4.3.1   Notification of Card Use Restrictions

An Issuer must include language in its Cardholder agreement that a Card must not be used for any unlawful purpose, including the purchase of goods or services prohibited by applicable laws or regulations.

ID# 0000386	Edition: Apr 2020	Last Updated: Oct 2014

1.4.3.2   International Transaction or Currency Conversion Fee Disclosure

An Issuer must provide a complete written disclosure of any fees that may be charged to a Cardholder for an International Transaction or when Currency Conversion occurs and must include the exchange rate between the Transaction Currency and the Billing Currency as either of the following:

- A rate selected by Visa from the range of rates available in wholesale currency markets for the applicable Processing Date, which rate may vary from the rate Visa receives
- The rate mandated by a government or governing body in effect for the applicable Processing Date[1]

When Currency Conversion occurs, the Visa rate may be adjusted by the application of an Optional Issuer Fee as determined by the Issuer or via any Issuer self-determined markup outside of VisaNet.

An Issuer may choose the method by which it notifies the Cardholder. This may include one or more of the following, which may include electronic forms of communication:

- Original Cardholder application agreement

- Terms and conditions

- Billing statement

- Any other agreement between the Cardholder and the Issuer

[1] This does not apply in the Canada Region, where Issuers must disclose the fact that the Currency Conversion rate is provided by Visa, and then marked up accordingly by the Issuer if it chooses to add such a markup.

ID# 0000387	**Edition: Apr 2020	Last Updated: Apr 2017**

1.4.3.3   Required Data on Cardholder Billing Statement

An Issuer must include on the Cardholder billing statement all of the following:

- The data transmitted in the Clearing Record that both:

  - Identifies one of the following, as applicable:

    ▪ The Merchant

    ▪ The Sponsored Merchant and its Payment Facilitator

    ▪ The Staged Digital Wallet Operator and retailer

  - Enables the Cardholder to contact the Merchant[1]

- The Issuer name, in a prominent position

- In the Europe Region (United Kingdom): The Airline Ticket Identifier, where it has been provided in the Merchant name field of the Clearing Record

[1] In the Europe Region: The Clearing Record for an Intraregional Recurring Transaction must contain either an Electronic Commerce Merchant's website address in the Merchant name field or, for all other Merchants, an internationally accessible telephone number in the Merchant city field.

ID# 0004080	**Edition: Apr 2020	Last Updated: Oct 2017**

1.4.3.4   Cardholder Signature on Card

When an Issuer issues or reissues a Card that has a signature panel, the Issuer must:

- Advise the Cardholder to immediately sign the signature panel on the Card

- Indicate that the Card must be signed in order to be valid

ID# 0025977	**Edition: Apr 2020	Last Updated: Oct 2019**

1.4.3.5 Disclosure of Visa Transaction Information – US Region

In the US Region: An Issuer may only disclose Visa Transaction Information to third parties approved by Visa and for the sole purpose of:

- Supporting a loyalty program
- Providing fraud control services

This does not apply to a Visa Commercial Card Issuer.

ID# 0003555   Edition: Apr 2020 | Last Updated: Oct 2015

1.4.4 Issuer Operational Standards

1.4.4.1 PIN Issuance

An Issuer must make a PIN available to each Cardholder for use with a Card, except as approved otherwise for one of the following:

- Emergency Card Replacement
- Non-Reloadable Prepaid Card
- Prepaid Card where cash access is restricted

ID# 0004019   Edition: Apr 2020 | Last Updated: Apr 2020

1.4.4.2 PIN Issuance Requirements

An Issuer must:

- Notify its Cardholders of PIN availability. In the Europe Region, an Issuer will be subject to a non-compliance assessment if it does not issue PINs to at least 75% of its Cardholders, or, if it did not issue a PIN, notify those Cardholders that they may select their own PINs, or request that a PIN be issued.

- Successfully complete certification testing to demonstrate its capability to perform PIN Verification, or designate Visa to perform this function

- Ensure the security of the PIN

- Select Stand-In Processing Issuer options pertaining to a Transaction for which a PIN is used. In the Europe Region, an Issuer must communicate these options to Visa.

- In the US Region: Notify its Cardholders of the availability of the Visa ATM Network. An Issuer must provide the notification annually to all active Cardholders of all of the following:

– Visa Check Card

– Visa Signature

– Visa Signature Preferred

ID# 0004571	Edition: Apr 2020 | Last Updated: Oct 2016

1.4.4.3 Issuer Responsibility for Stand-In Processing Authorizations

An Issuer is responsible for a Transaction authorized by Stand-In Processing.

ID# 0004386	Edition: Apr 2020 | Last Updated: Oct 2014

1.4.4.4 Issuer Credit Transaction Posting

In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: An Issuer must post a Credit Transaction Receipt to a Cardholder's account within 5 calendar days from the Settlement date.

In the US Region: An Issuer must post a Credit Transaction Receipt to a Cardholder's account:

- For Credit Cards, within 3 business days from the Settlement date
- For Visa Check Cards, within 1 business day of Settlement, unless circumstances or account history warrant a delay
- For Prepaid Cards, within 1 business day of Settlement, unless circumstances or account history warrant a delay

ID# 0025743	Edition: Apr 2020 | Last Updated: Apr 2020

1.4.4.5 VisaNet Issuer Billing Currency Selection Requirements

An Issuer must ensure that the Billing Currency designated in VisaNet is the same currency in which the Cardholder is debited[1] for Transactions, or in which the Issuer bills and receives payment for Cardholder Transactions.

If an Issuer offers multiple currencies for billing and/or payment, the default Billing Currency must be the national currency.[2]

[1] The Billing Currency designated in VisaNet must match the currency of the underlying account or source of funds.

[2] This does not apply to Cards enabled with the Visa Multi-Currency Solution, travel Prepaid Cards (including Visa TravelMoney), or Centralized Card Issuance.

ID# 0029503	Edition: Apr 2020 | Last Updated: Apr 2020

1.4.4.6   Cardholder Account Currency

Any non-fiat currency funds must be converted to a fiat currency before deposit into a Cardholder account linked to a Prepaid Card or Debit Card.[1] Conversion of non-fiat currency funds must be carried out in accordance with applicable laws in the country of issuance.

The Issuer must receive Visa approval before implementing a Visa Program linked to a Cardholder account that accepts deposited funds that were previously converted from a non-fiat currency.

An Issuer must not claim that a Visa product is directly linked to or funded by an account containing a non-fiat currency.

[1] An account linked to a Credit Card must not be funded via such a conversion or by a non-fiat currency.

ID# 0030097	Edition: Apr 2020 | Last Updated: Apr 2020

1.4.6   Zero Liability

1.4.6.1   Zero Liability

An Issuer must limit a Cardholder's liability to zero upon notification from the Cardholder of an unauthorized Transaction.

The limitation of liability does not apply to the following:

- Visa Corporate Card Transactions
- Visa Purchasing Card Transactions
- Anonymous Prepaid Card Transactions

The Issuer may increase the amount of the Cardholder's liability for unauthorized Transactions if the Issuer reasonably determines, based on substantial evidence, that the Cardholder was fraudulent or negligent in the handling of the account or the Card.

The Issuer must communicate any restrictions to its Cardholders.

In the Europe Region: An Issuer must limit a Cardholder's liability to zero upon notification from that Cardholder of an unauthorized Transaction.

The limitation of liability does not apply to the following:

- Visa Corporate Card Transactions
- Visa Purchasing Card Transactions
- Anonymous Prepaid Card Transactions

The Issuer may increase the amount of the Cardholder's liability for unauthorized Transactions if the Issuer reasonably determines, based on substantial evidence, that either or both:

- The Cardholder has acted fraudulently or negligently in the handling of the account or the Card.
- The Cardholder is proven to have participated in the Transaction.

The Issuer must communicate any restrictions to its Cardholders.

ID# 0029460	**Edition: Apr 2020 | Last Updated: Apr 2020**

1.5   Acceptance

1.5.1   General Acquirer Requirements

1.5.1.1   Acquirer Jurisdiction and Restriction of Cross-Border Acquiring

An Acquirer must accept and submit Transactions into Interchange only from Merchants, Marketplaces, Payment Facilitators, Sponsored Merchants, and Staged Digital Wallet Operators within that Acquirer's jurisdiction.

An Acquirer must accept Transactions only from a Merchant Outlet within the Acquirer's Country of Domicile (and that country's territories and possessions) unless any of the following:

- The Acquirer is licensed by Visa to accept Transactions from a Merchant Outlet in another country. In the Europe Region: A Transaction must be deposited in the Transaction Country.
- The Merchant is an Airline[1] or an on-board service provider contracted by the Airline[2] and the Acquirer maintains the relationship in accordance with the provisions of the International Airline Program.[3]
- The Merchant Outlet is, or is located in or on the premises of, a military base, embassy, or consulate or international governmental organization (for example: the United Nations) on foreign territory.[2]
- In the Europe Region: An Acquirer has passported its license in line with EU passporting regulations.

A Payment Facilitator must not contract with a Sponsored Merchant that is outside the country in which the Payment Facilitator and its Acquirer are located.

In the Europe Region: A Payment Facilitator located in a Europe Region country may contract with a Sponsored Merchant located in another Europe Region country only if both the Payment Facilitator and its Acquirer have appropriate business licenses for that country.

In the Canada Region, US Region: An Acquirer may cross-border acquire Electronic Commerce Transactions and Mail/Phone Order Transactions only as follows:

Table 1-7: Permitted Cross-Border Acquiring

Acquirer Region	Merchant Region	Cardholder Region	Currency Used in Advertising and Transaction Processing
Canada	US	Canada	CAD
US	Canada	US	USD

Visa may determine the country of a Merchant Outlet and an Acquirer's ability to contract with it based on an evaluation of the Merchant's business structure and any other information. A decision by Visa is final.

[1] For the purchase of travel or lodging at a travel agency, the Transaction Country is the country in which the travel agency is located.

[2] Such a Merchant may contract with an Acquirer that is licensed in the Merchant's home country, the Merchant Outlet Country, or both.

[3] The Acquirer must pay the domestic Interchange Reimbursement Fee (IRF) when entering a domestic Airline Transaction Receipt into international Settlement.

ID# 0008552   **Edition: Apr 2020 | Last Updated: Apr 2020**

1.5.1.2   Assignment of Merchant Outlet Location

An Acquirer must assign the correct location of its Merchant's Merchant Outlet. An Acquirer must not misrepresent or alter, or allow its Merchant or agent to misrepresent or alter, a Merchant Outlet location.

For a Card-Present Environment Transaction, the Acquirer must assign the following as the Merchant Outlet location:

Table 1-8: Allowed Merchant Outlet Locations for Card-Present Transactions

Transaction	Merchant Outlet location for that Transaction must be:
Transaction at a Merchant Outlet in a fixed location	Location at which the Transaction is completed
In-Transit Transaction	One of the following: • The location where the journey originated

Table 1-8: Allowed Merchant Outlet Locations for Card-Present Transactions (continued)

Transaction	Merchant Outlet location for that Transaction must be:
	• An interim or the final destination • The location of the Merchant's Principal Place of Business
Transaction at a Merchant Outlet not in a fixed location[1]	Either: • The location at which the Transaction is completed • The location of the Merchant's Principal Place of Business

For a Card-Absent Environment Transaction, the Acquirer must assign the country of the Merchant's Principal Place of Business[2] as the Merchant Outlet location. The Acquirer may assign additional Merchant Outlet locations if the Transaction is one of the following:

Table 1-9: Allowed Additional Merchant Outlet Locations for Card-Absent Transactions

Transaction	Additional Merchant Outlet location may be:
Transaction at an Airline,[2] passenger railway Merchant,[2] Cruise Line,[2] or other travel Merchant[2]	The country from which the first leg of the purchased travel originates
Transaction at a Lodging Merchant[2]	The country in which the Cardholder's stay occurs
Transaction at a Vehicle Rental Merchant,[2] taxi Merchant, or ride service Merchant	The country in which the Cardholder rents the car or the journey originates
Transaction at any other Merchant	The country in which all of the following occur,[3] as specified in the *Visa Merchant Data Standards Manual:*[4] • The Merchant has a permanent location at which the Merchant's employees or agents conduct the business activity directly related to the provision to the Cardholder of the goods or services purchased in the specific Transaction.

Table 1-9: Allowed Additional Merchant Outlet Locations for Card-Absent Transactions (continued)

Transaction	Additional Merchant Outlet location may be:
	• The Merchant assesses sales taxes on the Transaction activity. • The location is the legal jurisdiction, for the Transaction, that governs the contractual relationship between the Merchant and the Cardholder as the purchaser of the goods or services.

If Visa disputes a Merchant Outlet location assigned by an Acquirer, the correct location of the Merchant Outlet may be determined by Visa in its sole discretion.

[1] A location (or locations) at which a Merchant completes Transactions and is not the fixed or permanent premises of the Merchant. This does not apply to a mobile Acceptance Device within a fixed Merchant Outlet.

[2] For the purchase of travel or lodging at a travel agency, the Merchant Outlet location must be the country in which the travel agency is located.

[3] In the Europe Region: An exception applies to Merchant Outlet locations within the European Economic Area.

[4] If a Card-Absent Merchant (except a travel/lodging Merchant) qualifies for one or more additional Merchant Outlet locations, the Acquirer may assign the location for a Transaction only as the location where the underlying business activity occurs for the specific Transaction (either the Principal Place of Business or a qualifying additional Merchant Outlet location).

ID# 0029455   **Edition: Apr 2020 | Last Updated: Oct 2017**

1.5.1.3   Merchant Qualification Standards

Before entering into a Merchant Agreement, an Acquirer or a Payment Facilitator must ensure that the prospective Merchant is all of the following:

• Financially responsible

• Not engaged in any activity that could cause harm to the Visa system or the Visa brand

• Operating within an allowed jurisdiction

• Not misrepresenting its Merchant Outlet location or locations

The Acquirer or Payment Facilitator must also determine that there is no significant derogatory background information about any of the Merchant's principals.

ID# 0008478   **Edition: Apr 2020 | Last Updated: Apr 2017**

1.5.1.4   Submission of Illegal Transactions

An Acquirer must not knowingly accept from a Merchant for submission into the Visa payment system any Transaction that is illegal or that the Acquirer or Merchant should have known was illegal.

ID# 0028040	Edition: Apr 2020 | Last Updated: Oct 2014

1.5.1.5   Acquirer Use of Digital Certificates

An Acquirer that issues Digital Certificates to its Merchants or Payment Facilitators to enable them to access Visa-owned system components must use only Digital Certificates associated with Visa.

ID# 0004617	Edition: Apr 2020 | Last Updated: Oct 2014

1.5.1.6   Security of Payment Credentials and Payment Account References

An Acquirer must ensure all of the following:

- That the Account Number associated with a Token in a Transaction is not disclosed to the Merchant
- That a Payment Account Reference (PAR) is not stored with its associated full Payment Credential
- That a Transaction is not initiated with a PAR
- That a PAR is used only for the following:
  - Providing or managing customer service
  - Performing fraud and risk control activities
  - Supporting value-added services in which the Cardholder has opted to participate
  - Aiding compliance with applicable laws or regulations

ID# 0029276	Edition: Apr 2020 | Last Updated: Apr 2020

1.5.1.7   Authorization Rejection Based on Internal Tables

A Member must not selectively reject or decline Authorization Requests based on an internally developed table of BINs or Account Numbers.

This prohibition both:

- Includes tables developed using any table or file that includes BIN Attributes

- Does not include Authorization Requests originating from a Limited Acceptance Merchant for Account Numbers that contain a BIN not accepted by the Merchant

ID# 0008817	Edition: Apr 2020 | Last Updated: Apr 2020

1.5.1.8   Acquirer Rights to Provide Merchant Information

An Acquirer, a Marketplace, a Payment Facilitator, or a Digital Wallet Operator must ensure that it has all necessary and appropriate rights under applicable laws or regulations, privacy policies, or agreements to provide Merchant or retailer information to Visa.

ID# 0026459	Edition: Apr 2020 | Last Updated: Apr 2018

1.5.1.9   Termination of Merchant Agreement

After verifying that Visa has prohibited a Merchant, Sponsored Merchant, or Payment Facilitator from participating in the Visa or Visa Electron Program, an Acquirer must terminate the Merchant Agreement or Payment Facilitator Agreement no later than the date specified by Visa.

If the Acquirer does not terminate the Merchant Agreement or Payment Facilitator Agreement by the specified date, Visa may assess the Acquirer a non-compliance assessment.

An Acquirer or Payment Facilitator that enters into a Merchant Agreement with a Merchant, Sponsored Merchant, or known principals of a Merchant or Sponsored Merchant that Visa has prohibited from participating in the Visa Program or Visa Electron Program may be assessed a non-compliance assessment.

ID# 0008241	Edition: Apr 2020 | Last Updated: Oct 2015

1.5.2   Merchant Agreements

1.5.2.1   Merchant Agreement Requirements

An Acquirer must have a Merchant Agreement with each of its Merchants to accept Visa Cards and, if applicable, Visa Electron Cards. A Payment Facilitator must have a Merchant Agreement with each of its Sponsored Merchants.

The Merchant Agreement must include language that requires the Merchant to do all of the following:

- Perform its obligations under the Merchant Agreement in compliance with applicable laws or regulations

- Comply with the Visa Rules regarding use of the Visa-Owned Marks, Visa acceptance, risk management, Transaction processing, and any Visa products, programs, or services in which the Merchant is required to, or chooses to, participate

- Not knowingly submit any Transaction that is illegal or that the Merchant should have known was illegal

- Include the right of Visa to limit or terminate the Acquirer's agreement with the Merchant or the Payment Facilitator's agreement with the Sponsored Merchant

An Acquirer and a Payment Facilitator may accept Transactions only from an entity with which it has a valid Merchant Agreement.

ID# 0003356	Edition: Apr 2020 | Last Updated: Oct 2015

1.5.3   Marks Display

1.5.3.1   Display of Card Acceptance Marks

A Member or Merchant must display the appropriate Visa-Owned Marks to indicate which Cards it accepts for payment.

An Acquirer must ensure that each of its Limited Acceptance Merchants displays the appropriate Visa-Owned Marks to indicate only the Cards that it accepts for payment in accordance with its Merchant Agreement. A Limited Acceptance Merchant must not display any Visa graphic that indicates acceptance of all Visa Cards.

ID# 0008496	Edition: Apr 2020 | Last Updated: Apr 2018

1.5.4   Card Acceptance

1.5.4.1   Accepting Visa Products for Payment

Visa Merchants displaying Visa acceptance Marks at payment locations agree to accept corresponding Visa-branded products for payment. If the customer indicates that he or she wants to pay with a Visa product, a Merchant must complete and process the Visa Transaction as defined in the Visa Rules.

ID# 0007777	Edition: Apr 2020 | Last Updated: Apr 2018

Visa Core Rules and Visa Product and Service Rules

1.5.4.2   Honor All Cards

A Merchant must accept all Cards[1] properly presented for payment.

This does not apply to the following, where limited acceptance is permitted:

- Merchant Outlets that deploy Contactless-only Acceptance Devices, as specified in *Section 5.7.2.2, Deployment of Contactless-Only Acceptance Devices*

- Merchants that accept only Mobile Push Payment Transactions. Such Merchants must accept all Mobile Push Payment Transactions (except Cash-In and Cash-Out Transactions, which the Merchant may choose to accept)

- In the AP Region (Australia), Canada Region, US Region: Certain categories of Visa products for domestically issued Cards

- In the Europe Region: A Merchant in the European Economic Area (EEA), for certain Product Categories, as specified in *Section 1.5.4.6, Limited Acceptance Merchant Requirements – Europe and US Regions*

A Merchant may not refuse to accept a Visa product that is properly presented for payment (for example: a Card that is foreign-issued[2,3] or co-branded with the Merchant's competitor's Mark).

A Merchant may attempt to steer customers who initially present a Visa Card to an alternative method of payment, but may not do so in a manner that denies consumer choice.

A Merchant may also consider whether present circumstances create undue risk (for example: if the sale involves high-value electronics but the Card signature panel is not signed, and the Cardholder does not have any other identification).

[1] Based on the technology supported by the Merchant

[2] In the AP Region (Australia), Canada Region, US Region: A Merchant may decline to accept certain categories of Visa products for domestically issued Cards.

[3] In the Europe Region: A Merchant in the European Economic Area (EEA) may decline to accept certain Product Categories.

ID# 0008591   **Edition: Apr 2020 | Last Updated: Oct 2018**

1.5.4.3   Honor All Cards – Canada Region

In the Canada Region: Unless a Merchant has elected to not be a Visa Debit Acceptor, a Merchant that accepts Visa Cards must accept any valid Visa Card that a Cardholder properly presents for payment. This means that the Merchant must permit the Cardholder to choose whether to pay for a transaction with that Visa Card or with some other means of payment accepted by the Merchant.

Merchants that have elected to be a Visa Debit Acceptor may choose whether or not to accept domestic Visa Credit Cards. Similarly, Merchants that have elected to be a Visa Credit Acceptor may choose whether or not to accept Visa Debit Category Cards issued by Canada Issuers.

If a Cardholder presents a Visa Card that bears a Mark representing another payment service, the Merchant may not intentionally mislead the Cardholder concerning what payment service or system will be used. If the Merchant provides any information regarding the customer's rights related to various transaction choices, that information must be accurate.

ID# 0008392   Edition: Apr 2020 | Last Updated: Apr 2018

1.5.4.4   Honor All Cards – US Region

In the US Region: A Merchant that wishes to accept Visa Cards must accept any valid Visa Card in its category of acceptance that a Cardholder properly presents for payment. This means that the Merchant must permit the Cardholder to choose whether to pay for a transaction with that Visa Card or with some other means of payment accepted by the Merchant. The Merchant may request or encourage a Cardholder to use a means of payment other than a Visa Card.

ID# 0002867   Edition: Apr 2020 | Last Updated: Apr 2018

1.5.4.5   Selection of Payment System – Europe and US Regions

In the Europe Region: At a Merchant in the European Economic Area (EEA), if a Cardholder presents a Card that is issued in the EEA and that is co-badged with another payment scheme accepted by the Merchant, the Merchant must both:

- Honor the Cardholder's choice of payment scheme
- Process the transaction according to the Cardholder's choice of payment scheme

In the US Region: If a Cardholder presents a Visa Card[1] that is in the Merchant's category of acceptance and that bears a Mark representing another payment service:

- The Merchant must honor the Cardholder's request if the Cardholder indicates that the transaction is to be processed as a Visa Transaction.
- The Merchant may process the transaction as something other than a Visa Transaction despite an initial indication by the Cardholder that the transaction is to be processed as a Visa Transaction, but only if the Cardholder agrees that the transaction may be processed as something other than a Visa Transaction. The Merchant may not mislead the Cardholder concerning what payment service or system will be used. If the Merchant provides any information regarding the customer's rights related to various transaction choices, that information must be accurate.

[1] In the US Region or a US Territory: This does not apply to a US Covered Visa Debit Card.

1.5.4.6   Limited Acceptance Merchant Requirements – Europe and US Regions

In the Europe Region, US Region: A Merchant that accepts Visa Cards may choose Limited Acceptance.

Effective through 17 April 2020 In the Europe Region: A Limited Acceptance Merchant in the European Economic Area (EEA) must both:

- Accept all Cards that carry the Product Categories accepted by the Merchant
- Accept any valid Card issued by an Issuer outside the EEA

Effective 18 April 2020 In the Europe Region: A Limited Acceptance Merchant must not discriminate between Issuers within any Product Category it accepts. If a Limited Acceptance Merchant in the European Economic Area (EEA) selects to only accept certain Product Categories, then the following applies:

- If a Limited Acceptance Merchant accepts Credit Cards, the Limited Acceptance Merchant must accept all Credit Cards issued in the EEA.
- If a Limited Acceptance Merchant accepts Debit Cards, the Limited Acceptance Merchant must accept all Debit Cards issued in the EEA.
- If a Limited Acceptance Merchant accepts Prepaid Cards, the Limited Acceptance Merchant must accept all Prepaid Cards issued in the EEA.
- A Limited Acceptance Merchant is not required to accept commercial Cards issued in the EEA.

A Limited Acceptance Merchant must accept any valid Card issued outside the EEA.

In the US Region: A Merchant that accepts all Cards or a Limited Acceptance category of Cards must accept any valid Card issued by a non-US Issuer, as specified in the Visa Rules.

1.5.4.7   Limited Acceptance Notification Requirements – Europe and US Regions

In the Europe Region: An Acquirer must register with Visa each of its Limited Acceptance Merchants.

In the US Region: An Acquirer must register with Visa and provide reporting on any Merchant that elects to be a Limited Acceptance Merchant.

1.5.4.8 Chip Card Acceptance Requirements

The Card and Cardholder must be present for all Chip-initiated Transactions.

If a Chip-initiated Transaction is declined by the Issuer, the Transaction must not be processed by any other means.

ID# 0004845	Edition: Apr 2020 | Last Updated: Oct 2014

1.5.4.9 Visa Mini Card Merchant Acceptance Requirements

A Merchant that accepts Cards must both:

- Attempt to accept a Visa Mini Card
- Request a corresponding standard-sized Card, if available, if either the:
  - Acceptance Device is unable to read the Magnetic Stripe on the Visa Mini Card
  - Full Account Number is not placed on the Visa Mini Card

ID# 0027521	Edition: Apr 2020 | Last Updated: Apr 2020

1.5.4.10 Uniform Services – Acquirer Requirements

An Acquirer must both:

- Accept all Cards properly presented for payment
- Offer and render services uniformly to all Cardholders[1]

This does not apply to Contactless-only Acceptance Devices, as specified in *Section 5.7.2.2, Deployment of Contactless-Only Acceptance Devices.*

[1] This does not apply to discounts, promotional offers, or in-kind incentives offered by the Merchant.

ID# 0005302	Edition: Apr 2020 | Last Updated: Apr 2016

1.5.4.11 Uniform Services – Merchant Requirement

A Merchant must process Transactions with all Cardholders in exactly the same manner.

This does not apply to discounts, promotional offers, or in-kind incentives offered by the Merchant to a subset of Visa Cards.

ID# 0003018	Edition: Apr 2020 | Last Updated: Oct 2018

1.5.4.12   Discount Offer – US Region and US Territories

In the US Region and a US Territory: A Merchant may request or encourage a Cardholder to use a means of payment other than a Visa Card or a Visa Card of a different product type (for example: Visa Classic Card, Visa Traditional Rewards Card, Visa Signature Card) than the Visa Card the consumer initially presents. Except where prohibited by applicable laws or regulations, the Merchant may do so by methods that include, but are not limited to:

- Offering the consumer an immediate discount from the Merchant's list, stated, or standard price, a rebate, a free or discounted product or service, or any other incentive or benefit if the consumer uses a particular general purpose payment card with an acceptance brand other than a Visa Card or other particular means of payment

- Offering the consumer an immediate discount from the Merchant's list, stated, or standard price, a rebate, a free or discounted product or service, or any other incentive or benefit if the consumer, who initially presents a Visa Card, uses instead another general purpose payment card or another means of payment

- Expressing a preference for the use of a particular general purpose payment card or means of payment

- Promoting the use of a particular general purpose payment card with an acceptance brand other than Visa or means of payment through posted information, through the size, prominence, or sequencing of payment choices, or through other communications to consumers

- Communicating to consumers the reasonably estimated or actual costs incurred by the Merchant when a consumer uses a particular general purpose payment card or means of payment or the relative costs of using different general purpose payment cards or means of payment

ID# 0008590   **Edition: Apr 2020 | Last Updated: Oct 2014**

1.5.4.13   Acquirer Requirements – Discount at the Point of Sale – US Region and US Territories

In the US Region or a US Territory: An Acquirer must not adopt, maintain or enforce any rule (including any bylaw, policy, standard, guideline, or practice), or enter into or enforce any agreement that directly or indirectly prohibits, prevents, or restrains its Merchants from requesting or encouraging a Cardholder to use a means of payment other than a Visa Card or a Visa Card of a different product type (e.g., Visa Classic Card, Visa Traditional Rewards Card, Visa Signature Card) than the Visa Card the consumer initially presents. The methods by which a Merchant may request or encourage a Cardholder to use a means of payment other than a Visa Card or a Visa Card of a different product type include but are not limited to the methods specified in *Section 1.5.4.12, Discount Offer – US Region and US Territories*.

An Acquirer may enforce agreements or enter into agreements with its Merchants where the Merchant selects Visa Cards as the only general purpose payment cards the Merchant will accept.

ID# 0026490	Edition: Apr 2020 | Last Updated: Oct 2014

1.5.4.14   Incentive to Use Other Payment Method – US Region

In the US Region: A Merchant may offer a non-monetary benefit to a Cardholder as an inducement for the Cardholder to use a means of payment other than a Visa Card.

A Merchant may offer a monetary benefit in the form of a discount, as specified in _Section 1.5.4.12, Discount Offer – US Region and US Territories,_ as an inducement for the Cardholder to use a means of payment other than a Visa Card.

ID# 0002870	Edition: Apr 2020 | Last Updated: Oct 2014

1.5.4.15   Credit Refund Requirements

A Merchant may establish its own credit refund policy, but must disclose it as specified in _Section 5.4.2.4, Disclosure to Cardholders of Return, Refund, and Cancellation Policies_

A Merchant must not:

- Accept payment from a Cardholder for the purpose of depositing funds to the Cardholder's account[1]
- Process a Credit Transaction Receipt without having completed a previous retail Transaction with the same Cardholder

These restrictions do not apply to:

- The loading of value to a Prepaid Card that participates in the Visa Prepaid Load Service
- In the US Region: The loading of value to a Prepaid Card or to another non-Visa-branded account that participates in Visa ReadyLink

If a Merchant provides a refund to a Cardholder for a previous purchase, the following conditions apply:

- To the extent possible, the Merchant must process a Credit Transaction[2] to the same Payment Credential as used in the original Transaction.
- If unable to process the Credit Transaction to the same Payment Credential, the Merchant may either:
  - Process the Credit Transaction to a secondary Payment Credential, if available, and if a Transaction Receipt or other proof of purchase exists, and either:

- The original Payment Credential is unavailable (account is closed, transferred, reported lost/stolen).

- An Authorization Request for the Credit Transaction[2] to the original Payment Credential receives a Decline Response.

  – Refund the Transaction amount through alternate means (cash, check, in-store credit, or prepaid card), if any of the following conditions apply:

  - The Cardholder does not have a Transaction Receipt or other proof of purchase.

  - The customer is not the original Cardholder and is returning a gift.

  - The Cardholder claims that the Prepaid Card used for the original purchase has been discarded.

  - The Authorization Request for a Credit Transaction to the original or secondary Payment Credential receives a Decline Response.

In the AP Region (Australia, New Zealand), Europe Region, US Region, US Territory: The Merchant must refund any surcharge[3] assessed on the Transaction amount. For partial refunds, the surcharge[3] amount must be pro-rated.

[1] Except a Cash-In Transaction

[2] This does not apply to a Straight Through Processing Transaction.

[3] In the AP Region (Australia): A Surcharge. In the US Region, US Territory: A US Credit Card Surcharge.

| ID# 0003076 | Edition: Apr 2020 \| Last Updated: Apr 2020 |

1.5.5   Card Acceptance Prohibitions

1.5.5.1   Prohibition of Minimum or Maximum Transaction Amount

A Merchant must not establish a minimum or maximum Transaction amount as a condition for honoring a Card.

This does not apply to a European Economic Area Transaction.

This does not apply to a Transaction initiated with a Credit Card issued in the US Region or a US Territory used at a Merchant Outlet in the US Region or a US Territory, as specified in *Section 5.4.2, Conditions of Card Acceptance and Cardholder Rights*

| ID# 0026405 | Edition: Apr 2020 \| Last Updated: Apr 2020 |

1.5.5.2   Surcharges

A Merchant must not add any amount over the advertised or normal price to a Transaction, unless applicable laws or regulations expressly require that a Merchant be permitted to impose a surcharge. Any surcharge amount, if allowed, must be included in the Transaction amount and not collected separately.

In the AP Region (New Zealand): This does not apply under certain terms and conditions, as communicated to Members. Further information is available from Visa.

In the US Region and US Territories: This does not apply to Credit Card Transactions, as specified in *Section 5.6.1.5, US Credit Card Surcharge Requirements – US Region and US Territories.*

In the Europe Region: The Merchant must clearly communicate any surcharge amount to the Cardholder, and the Cardholder must agree to the surcharge amount, before the Merchant initiates the Transaction.

ID# 0006948	Edition: Apr 2020 | Last Updated: Apr 2020

1.5.5.3   Cardholder Identification

Unless specified in the Visa Rules, a Merchant must not request Cardholder identification as a condition of purchase.

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Merchant that suspects fraud in a Face-to-Face Environment may request Cardholder identification. If the identification is expired or does not match the name on the Card, or if the Cardholder does not provide identification, the Merchant may decide whether to accept the Card.

ID# 0027481	Edition: Apr 2020 | Last Updated: Apr 2018

1.5.5.4   PIN Disclosure

A Merchant must not ask a Cardholder to reveal the Cardholder's PIN.

ID# 0008977	Edition: Apr 2020 | Last Updated: Oct 2018

1.5.5.5   Scrip Prohibition

An Acquirer or Merchant must not accept a Card for the purchase of Scrip, except in Sub-Saharan Africa.[1]

[1] Angola, Botswana, Comoros, Eritrea, Eswatini, Ethiopia, Gambia, Ghana, Kenya, Lesotho, Liberia, Malawi, Mauritius,

Mozambique, Namibia, Nigeria, Rwanda, Sierra Leone, Somalia, Seychelles, Sudan, Tanzania, Uganda, Zambia, Zimbabwe. Includes: Mascarene Is., Rodrigues Is.

ID# 0008708	Edition: Apr 2020 | Last Updated: Apr 2020

1.5.5.6   Merchant Cash Disbursement Prohibition

A Merchant must not provide cash to a Cardholder unless the Merchant provides Cash-Back or Cash-Out or sells foreign currency.

In the AP Region (Nepal): This does not apply for a disbursement in local currency by a Merchant that is licensed to sell foreign currency.

In the CEMEA Region (South Africa): This does not apply.

ID# 0006952	Edition: Apr 2020 | Last Updated: Apr 2020

1.5.5.7   Prepaid Card Cash Redemption

A Prepaid Card must not be redeemed for cash by a Merchant that accepts the Prepaid Card.

ID# 0025713	Edition: Apr 2020 | Last Updated: Apr 2020

1.5.6   Card and Cardholder Verification Requirements

1.5.6.1   Authorized Card User

An Acquirer or a Merchant must validate that the presenter of a Card is authorized to use the Card, as specified in *Section 5.5.1.1, Card and Cardholder Validation in a Face-to-Face Environment*.

ID# 0028041	Edition: Apr 2020 | Last Updated: Oct 2014

1.5.7   Transaction Receipts

1.5.7.1   Cardholder Verification without Final Transaction Amount

A Merchant must not require a Cardholder to perform Cardholder Verification before the final Transaction amount is entered on the Transaction Receipt or displayed to the Cardholder. A Merchant may only perform Cardholder Verification before displaying the final Transaction amount for any of the following:

- A Merchant specified in *Section 5.8.3.1, Authorization Amount Requirements*. This in itself does not constitute Cardholder acceptance of the final Transaction amount.

- A Merchant that uses a Visa-approved "quick Chip" processing solution, where available, only if all of the following conditions are met:

  - The Merchant's POS system automatically calculates the final amount

  - The final amount is displayed and confirmed by the Cardholder before the Merchant submits an Authorization Request[1]

  - A fully itemized Transaction Receipt is offered to the Cardholder

[1] Except at a Merchant Outlet that receives or accepts tips.

ID# 0003120	Edition: Apr 2020 | Last Updated: Oct 2018

1.5.8 Merchant Deposits

1.5.8.1 Transaction Deposit Conditions

A Merchant, Payment Facilitator, Marketplace, or Staged Digital Wallet Operator must not submit a Deposit for a Transaction until one of the following occurs:

- The Transaction is completed.

- The merchandise or services are shipped or provided. This does not apply if the Cardholder has paid an Advance Payment.

- The Merchant, Sponsored Merchant, Marketplace or Staged Digital Wallet Operator has fulfilled the conditions of its agreement with the Cardholder for an Installment Transaction, a Recurring Transaction, or an Unscheduled Credential-on-File Transaction.

A Merchant, or Staged Digital Wallet Operator, must only submit a Deposit for a Transaction that it has completed with a Cardholder.

A Marketplace must only submit a Deposit for a Transaction between a Cardholder and a retailer that sells goods or services through the Marketplace.

A Payment Facilitator may only submit a Deposit for a Transaction between a Cardholder and a Sponsored Merchant of the Payment Facilitator, but must not submit a Deposit for a Transaction on behalf of another Payment Facilitator, Digital Wallet Operator, or Marketplace.

ID# 0002981	Edition: Apr 2020 | Last Updated: Oct 2019

1.5.8.2   Acquirer Payments to Card Acceptors

An Acquirer must pay or credit its Merchant's, Marketplace's, Sponsored Merchant's, Payment Facilitator's, or Staged Digital Wallet Operator's account promptly after Transaction Deposit. These payments must be the same as the Transaction totals, less any Credit Transaction Receipts, applicable discounts, Disputes, other agreed fees or Merchant reserve funds (if applicable) accumulated to guarantee the Merchant's, Sponsored Merchant's, Marketplace's, Payment Facilitator's, or Staged Digital Wallet Operator's payment system obligations to the Acquirer.

An Acquirer may directly pay or credit only:

- A Merchant

- A Payment Facilitator, on behalf of a Sponsored Merchant

- A Sponsored Merchant for its portion of the Deposit, if the Acquirer also contracts with the Payment Facilitator

- A Staged Digital Wallet Operator

- A Marketplace

If a Payment Facilitator receives payment from an Acquirer, it must pay or credit its Sponsored Merchant's account promptly after Transaction Deposit. These payments must be the same as the Transaction totals, less any Credit Transaction Receipts, applicable discounts, Disputes or other agreed fees.

A Marketplace must pay or credit its retailer's account promptly after Transaction Deposit. These payments must be the same as the Transaction totals, less any Credit Transaction Receipts, applicable discounts, Disputes or other agreed fees.

In the LAC Region (Brazil): An Acquirer or a Payment Facilitator must pay or credit its Merchant's or Sponsored Merchant's account, as follows:

- For domestic Credit Transactions, no later than 32 days after the Processing Date

- For all other Transactions, no later than 5 days after the Processing Date

ID# 0008850   **Edition: Apr 2020 | Last Updated: Oct 2019**

1.5.9   Travelers Cheques

1.5.9.1   Travelers Cheque Acceptance Requirements

A Member must accept and encash all Cheques denominated in currencies usually exchanged in the local market.

A Member's encashment policy must be as favorable for Cheques as for other cheque brands.

| ID# 0002657 | Edition: Apr 2020 \| Last Updated: Oct 2014 |

1.5.9.2 Travelers Cheque Acceptance Procedures

When encashing a Cheque, a Member must:

- Witness the customer countersigning the Cheque in the lower left signature area

- Compare the countersignature with the signature appearing in the upper right signature area. If the signatures appear similar, the Member may accept the Cheque.

If the Member is uncertain about the similarity of the signatures, it may request that the customer sign the Cheque on the back and provide identification. If the Member is satisfied with the identification comparison, it may accept the Cheque.

If a Cheque has already been countersigned, or if the presenter is not the original purchaser of the Cheque, the Member must only accept the Cheque if the presenter is a known customer and full recourse is available.

If the Cheque issuer does not honor a validly issued Cheque as a result of the issuer's financial condition or circumstances beyond the issuer's control, Visa guarantees reimbursement for the Cheque amount if the Member complies with the above encashment procedures.

| ID# 0008947 | Edition: Apr 2020 \| Last Updated: Oct 2015 |

1.6   ATM

1.6.1   ATM Requirements

1.6.1.1   Compliance with Visa Product and Service Rules: ATM

ATM rules are contained in *Visa Product and Service Rules: ATM*

| ID# 0028042 | Edition: Apr 2020 \| Last Updated: Oct 2014 |

1.7   Transaction Processing

1.7.1   General Processing

1.7.1.1   Authorization, Clearing, and Settlement of Transactions through VisaNet

A Visa participant must authorize, clear, and settle messages for international Visa Transactions through VisaNet, including those resulting from the use of restricted cards outside the country of issuance, and report to Visa all domestic Visa Transactions processed outside of VisaNet.

In some jurisdictions, except for those with processing exceptions approved by Visa, a participant must authorize, clear, and settle all Visa Transactions through VisaNet, which enhances Visa's ability to manage risks, meet consumer expectations, and provide leading fraud-protection solutions.

In the Canada Region: A Visa Debit Acquirer must process all Visa Debit Transactions through VisaNet.

In the Europe Region: For International Transactions that are European Economic Area Transactions, a Member will use a Visa Scheme Processor.

ID# 0007788	Edition: Apr 2020 | Last Updated: Oct 2019

1.7.1.2   BIN and Acquiring Identifier Processing Capability

A Member and VisaNet Processor must be capable of accepting and processing a BIN and an Acquiring Identifier for any Visa-defined purpose.

ID# 0008895	Edition: Apr 2020 | Last Updated: Oct 2019

1.7.2   Data Requirements

1.7.2.1   Complete and Valid Transaction Data

An Acquirer must ensure that all Authorization Requests and Clearing Records contain complete, accurate, and valid data.

If an Authorization is obtained, any data in the subsequent Clearing Record or Authorization Reversal must be the same as, or consistent with, comparable data in the Authorization Request and Authorization Response.

Effective 18 April 2020 In the Canada Region, Europe Region, LAC Region, US Region: An Acquirer, a Merchant, a Payment Facilitator, or a VisaNet Processor that reattempts an Authorization Request following a Decline Response, as specified in *Section 7.3.6.4, Declined Transaction Resubmission*

Requirements – Canada, Europe, LAC, and US Regions, must not intentionally manipulate any data elements from the original Authorization Request, including, but not limited to, the following:

- Acquiring Identifier
- Acquirer and Merchant country
- MCC
- POS condition code
- POS environment field
- POS Entry Mode
- Electronic Commerce Indicator

Merchant Outlet country data must be the same throughout the Transaction life cycle (including, but not limited to, an Authorization Request, the Clearing Record, and any subsequent Adjustment, Dispute, Credit Transaction, Authorization Reversal, or Reversal).

ID# 0008752	**Edition: Apr 2020 | Last Updated: Apr 2020**

1.7.3   Acquirer Authorization Requests

1.7.3.1   Required Authorization Processing through VisaNet

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: An Acquirer must process an Authorization for an International Transaction through VisaNet, as specified in *Section 1.7.1.1, Authorization, Clearing, and Settlement of Transactions through VisaNet.*

In the Europe Region: An Acquirer must process an Authorization for an Interregional Transaction through VisaNet, as specified in *Section 1.7.1.1, Authorization, Clearing, and Settlement of Transactions through VisaNet.* For International Transactions that are European Economic Area Transactions, a Member will use a Visa Scheme Processor.

ID# 0003369	**Edition: Apr 2020 | Last Updated: Oct 2019**

1.7.3.2   Authorization Currency and Conversion

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: An Authorization Request must be expressed only in USD, the Transaction Currency, or the local fiat currency.

If the Transaction Currency is not USD, an Acquirer may convert the Authorization amount into USD before sending the Authorization Request to Visa. If the Acquirer converts the Authorization amount, it must use a generally accepted wholesale currency market rate.

Visa Core Rules

1 Visa Core Rules

Visa Core Rules and Visa Product and Service Rules

An Acquirer must submit an Authorization Request for an ATM Cash Disbursement and a Manual Cash Disbursement in the Transaction Currency.

In the Europe Region: An Authorization Request must be expressed in the Transaction Currency.

ID# 0008803	Edition: Apr 2020 | Last Updated: Oct 2017

1.7.4   Issuer Authorization Processing

1.7.4.1   Issuer Requirement to Evaluate Each Transaction

An Issuer must evaluate each Transaction that has been properly accepted, processed, and submitted in order to make an Authorization, a Token provisioning,[1] or other decision, and must not block, refuse, or decline Authorization Requests, Token provisioning requests,[1] or Transactions in a systematic or wholesale manner,[2] unless there is an immediate fraud threat or an exception is otherwise specified by applicable laws or regulations or in the Visa Rules.[3]

In the LAC Region: This does not apply to a Card-Absent Environment Transaction conducted with a Visa Electron Card or an unembossed Debit Card issued in Argentina, Brazil, Chile, Colombia, Mexico, or Trinidad.

[1] Applies only to Visa Token Service participants and only to Stored Credential or Electronic Commerce enabler Tokens

[2] Including, but not limited to: by BIN, by geography, by payment channel, by payment device, by Transaction type

[3] An Issuer must send a Decline Response to an Authorization Request or a Token provisioning request if it has determined that the Transaction is illegal.

ID# 0029326	Edition: Apr 2020 | Last Updated: Apr 2020

1.7.4.2   Referral Responses – Prohibited Transaction Types

An Issuer must not send a referral response to an Authorization Request. In the event that an Issuer sends a referral response to such an Authorization Request, VisaNet will process the Authorization Request according to the Issuer's Stand-In Processing parameters.

ID# 0008832	Edition: Apr 2020 | Last Updated: Oct 2016

1.7.4.3   Reversal of Duplicate or Erroneous Authorizations

An Issuer must reverse a duplicate or erroneous Authorization Transaction from its Cardholder's account upon receipt of a Reversal.

ID# 0004383	Edition: Apr 2020 | Last Updated: Oct 2017

1.7.4.4   Issuer Authorization of Chip Fallback Transactions – Canada Region

In the Canada Region: An Issuer or the Issuer's agent must send a Decline Response to all Authorization Requests for domestic Chip Fallback Transactions.

ID# 0029999	Edition: Apr 2020 | Last Updated: Apr 2018

1.7.5   Clearing

1.7.5.1   Transaction Currency for Original Presentments

An Acquirer must enter all original Presentments into Interchange in the exact amount of Transaction Currency authorized by the Cardholder.

ID# 0008358	Edition: Apr 2020 | Last Updated: Oct 2014

1.7.5.2   Transaction Receiving Decline Response

Effective through 17 April 2020 An Acquirer may enter into Interchange a Transaction that has received a Decline Response only if either:

- The Transaction received a subsequent Approval Response to a new Authorization Request, and the Issuer did not send an Authorization Pickup Response of 04, 07, 41, or 43 for the account.

- The Transaction originated from a Mass Transit Merchant, as specified in *Section 7.3.6.3, Resubmission following a Decline Response to a Transit Transaction.*

Effective 18 April 2020 In the AP Region, CEMEA Region: An Acquirer may enter into Interchange a Transaction that has received a Decline Response only if either:

- The Transaction received a subsequent Approval Response to a new Authorization Request, and the Issuer did not send an Authorization Pickup Response of 04, 07, 41, or 43 for the account.

- The Transaction originated from a Mass Transit Merchant, as specified in *Section 7.3.6.3, Resubmission following a Decline Response to a Transit Transaction.*

ID# 0005701	Edition: Apr 2020 | Last Updated: Oct 2019

1.7.5.3   Transaction Receipts with Illegible or Invalid Payment Credentials

If an Acquirer that receives a Transaction Receipt with an illegible or invalid Payment Credential contacts the Issuer for assistance in obtaining the Payment Credential, the Issuer:

- Must assist the Acquirer

- May require that all requests be in writing

If the Acquirer is not able to identify the Issuer, the Acquirer that first received the Transaction Receipt is liable, unless the Acquirer can identify the Issuer within 12 months of the Transaction Date and clear the Transaction Receipt directly with the Issuer.

A Transaction processed under these procedures is not subject to Dispute Condition 12.1 (Late Presentment).

ID# 0029041	Edition: Apr 2020 | Last Updated: Apr 2020

1.7.6   Settlement

1.7.6.11   Reimbursement for Valid Transactions

An Issuer must pay the Acquirer the amount due for a Transaction occurring with the use of a valid Card. This includes Transactions resulting from geographically restricted Card use outside the country of issuance.

ID# 0006558	Edition: Apr 2020 | Last Updated: Oct 2014

1.7.7   Reversals and Adjustments

1.7.7.1   Online Financial Transaction Reversal Requirements

An Acquirer must process a Reversal for an Online Financial Transaction if either the:

- Acquirer, Merchant, or Acceptance Device did not receive an Authorization Response
- Transaction is subsequently voided or cancelled

ID# 0005477	Edition: Apr 2020 | Last Updated: Oct 2014

1.7.7.2   Transaction Processing Subsequent to an Authorization Reversal

A Merchant must not deposit, and an Acquirer must not process, a Transaction that either:

- Was subsequently reversed for the full amount
- Represents the amount of the partial Authorization Reversal

ID# 0025598	Edition: Apr 2020 | Last Updated: Oct 2014

1.7.7.3   Transaction Reversal or Adjustment

A Merchant must process a Reversal or an Adjustment within 30 calendar days[1] if it processed a Transaction in error.

[1] In the US Region: 45 calendar days for PIN-Authenticated Visa Debit Transactions

ID# 0008614	Edition: Apr 2020 | Last Updated: Oct 2016

1.7.7.4   Member Reversal of Duplicate or Erroneous Data

A Member that detects duplicate or erroneous data or is notified by Visa that it has processed such data must reverse the data and do all of the following:

- Identify the Processing Date of the Transaction that it is reversing
- Maintain all data from the duplicated or erroneous Transaction, except for the appropriate Reversal codes
- Send the Reversals to Visa (or, in the case of a Domestic Transaction under a Private Agreement, to the Receiving Member) within one business day of detection or notification of the duplicate or erroneous data

ID# 0008878	Edition: Apr 2020 | Last Updated: Oct 2017

1.7.7.5   Issuer Reversal of a Duplicate or Erroneous Transaction

An Issuer must reverse any duplicate or erroneous Transaction from its Cardholder's account upon receipt of Reversal information. Visa reverses the duplicate or erroneous Transaction using the Currency Conversion Rate effective on the Processing Date of the duplicate or erroneous data.

Visa assesses the responsible Members any foreign exchange loss due to currency fluctuation between the Processing Date of the duplicate or erroneous data and the Reversal date using the VisaNet fee collection process.

ID# 0008879	Edition: Apr 2020 | Last Updated: Oct 2017

1.7.7.6   Credit Reversals and Debit Adjustments

An Acquirer may initiate a credit Reversal only to correct inadvertent processing errors.

The Acquirer must process a credit Reversal or a debit Adjustment within 30[1] calendar days of the Processing Date of the initial Credit Transaction.

[1] In the US Region: 45 calendar days for PIN-Authenticated Visa Debit Transactions.

ID# 0008880	Edition: Apr 2020	Last Updated: Apr 2020

1.8   Processing Products

1.8.1   Original Credits

1.8.1.1   Original Credit Acceptance

A Member must accept an incoming Original Credit Transaction[1] unless prohibited by applicable laws or regulations.

If prohibited by applicable laws or regulations, the Member must submit a written request to Visa to block incoming Original Credit Transactions.

[1] Excluding all Non-Reloadable Prepaid Cards and Reloadable Prepaid Cards where Cardholder data is not on file or where the source of loads may be restricted (for example: government, healthcare, or insurance programs).

ID# 0004062	Edition: Apr 2020	Last Updated: Apr 2018

1.9   Interchange

1.9.1   Interchange Reimbursement Fee (IRF) Determination and Payment

1.9.1.2   What is Interchange? – AP, Canada, CEMEA, LAC, US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Interchange Reimbursement Fees (IRF) help to make electronic payments possible by enabling Visa to expand Card holding and use, increasing the places consumers can use their Cards, and providing a financial incentive for all parties to pursue system-wide improvements, such as rewards, innovation, and security. An Interchange Reimbursement Fee is a default transfer price between Acquirers and Issuers within the Visa system. Merchants pay what is known as a merchant discount fee or merchant service fee negotiated with their Acquirer, which may take into account the interchange fee, processing costs, fees for terminal rental, customer services, and other financial services. The merchant discount fee or merchant service fee is negotiated individually with the Merchant's Acquirer; each Acquirer sets its fees independently, in competition with other Acquirers, competing payment systems, and other forms of payment.

Interchange is consistently monitored and adjusted – sometimes increased and sometimes decreased – in order to ensure that the economics present a competitive value proposition for all parties. Interchange Reimbursement Fees must encourage Card holding and use, as well as expansion in the number and types of businesses that accept Cards. If rates are too high, retailers won't accept Cards; if rates are too low, Issuers won't issue Cards. Visa may establish different

Interchange Reimbursement Fees in order to promote a variety of system objectives, such as enhancing the value proposition for Visa products, providing incentives to grow merchant acceptance and usage, and reinforcing strong system security and Transaction authorization practices.

ID# 0024115	Edition: Apr 2020 | Last Updated: Oct 2017

1.9.1.3   Interchange Reimbursement Fee (IRF) Requirements

A Transaction must meet the qualifications defined in the Visa Rules and in the applicable Interchange Reimbursement Fee rate qualification guide to qualify for a particular Interchange Reimbursement Fee.

An Acquirer must also request the correct Interchange Reimbursement Fee, as applicable, when submitting a Transaction into Interchange.

ID# 0006611	Edition: Apr 2020 | Last Updated: Apr 2018

1.9.2   Interchange Reimbursement Fee (IRF) Adjustments and Compliance

1.9.2.1   Interchange Reimbursement Fee (IRF) Adjustments

If Interchange Reimbursement Fees are inappropriately received or paid by an Issuer or Acquirer, Visa reserves the right to rectify the improper allocations.

Interchange Reimbursement Fee adjustments may be made only as follows:

- Adjustments are limited to Transactions occurring within 90 calendar days of the Processing Date of the oldest Transaction submitted by the Member or identified by Visa.

- Transactions beyond 90 calendar days (not to exceed 2 years from the date submitted by the Member or identified by Visa) may be considered for adjustment if Visa determines that extenuating circumstances prevented the Member from discovering the violation sooner.

- When an Issuer or Acquirer is at fault, the impacted Issuer(s) or Acquirer(s) is required to use the Interchange Reimbursement Fee Compliance process.

- Adjustments will only be made when the total Interchange Reimbursement Fee amount to be corrected is greater than USD 2,500.

- Individual correcting Transactions will only be made if the amount of the correcting transaction is greater than USD 50.

Interchange Reimbursement Fee adjustments will be processed as follows:

- Visa will notify the Members that will receive a correcting Transaction.

- Visa will initiate a correcting Fee Collection Transaction (Transaction code 10) and Funds Disbursement Transaction (Transaction code 20) through VisaNet.

- All Visa decisions are final.

- A Member may appeal a decision only if the Member can provide new evidence not previously available and the amount in dispute is greater than USD 5,000.

Visa may, at its sole discretion, offer to use this adjustment process regardless of the adjustment amount.

ID# 0007972	**Edition: Apr 2020	Last Updated: Apr 2018**

1.9.2.2   Interchange Reimbursement Fee (IRF) Compliance Filing Requirements

A Member must not file for Interchange Reimbursement Fee (IRF) Compliance unless all of the following:

- A violation of the Visa Rules or any applicable regional or domestic Interchange Reimbursement Fee (IRF) guide occurred.

- The Member received or paid incorrect IRF as a direct result of the violation by another Member.

- The Member's financial loss is a direct result of an incorrectly applied IRF rate.

- The Member would not have incurred a financial loss if the violation had not occurred.

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: The violating Transactions were processed through VisaNet.

- The IRF rate paid or received is not governed by any bilateral or private agreements, either domestic, intraregional, or interregional.

- Visa has granted permission for the Member to file.

A Member may aggregate up to 1,000,000 Transactions into a single IRF Compliance case if the Transactions involved the same opposing Member and violated the same operating regulation or the same requirement in an applicable IRF guide. The value of the aggregated Transactions must not be less than the sum of the IRF screening fee and the IRF filing fee specified in the applicable regional fee guide.

Visa may refuse to allow a filing Member to participate in IRF Compliance. The decision by Visa to refuse participation is final and not subject to any challenge.

A Member must comply with the *Interchange Reimbursement Fee Compliance Process Guide*.

ID# 0001501	**Edition: Apr 2020	Last Updated: Oct 2017**

Visa Core Rules and Visa Product and Service Rules

1.10   Risk

1.10.1   Corporate Risk Reduction

1.10.1.2   Member Risk Reduction Requirements

Visa may impose conditions on a Member if it reasonably believes the Member's Visa Program is not being operated in a sound and safe manner or exposes Visa or its Members to financial loss.

Upon receipt of instructions imposing conditions, a Member or its agent must implement risk reduction measures that may include, but are not limited to, the following:

- Prohibiting or limiting any of the following actions:
  - Issuing new or reissued Cards
  - Signing or re-signing Merchants
  - Using an agent
- Blocking the Authorization of Transactions or prohibiting Acquirers from obtaining Authorization for Transactions on behalf of certain Merchants
- Terminating some or all Merchants that:
  - Conduct Transactions where the Cardholder is not present or where goods or services are to be delivered after the Transaction Date
  - Receive a volume of Disputes that substantially exceeds the system average
- Pledging collateral to secure one or more of the following:
  - A Member's or agent's obligations to Visa and reimbursement to Visa for any expenses incurred to ensure compliance
  - The liquidity impact to Visa of Settlement or other payments due to Visa from a Member, its affiliates, or its Clearing Processor as approved by Visa
  - Reimbursement to Visa for any expenses incurred to ensure compliance
- Consolidating into a single Funds Transfer Settlement Reporting Entity all or some of the Settlement payments in a Settlement Currency of a Member and its affiliates or of a Clearing Processor as approved by Visa for one or more Members arising from one or more Settlement systems operated by Visa or its subsidiaries or affiliates, operated privately, or by a third party, in order to reduce the liquidity impact of such Settlement payments on Visa (Settlement Payment Consolidation) or risk of Settlement Loss (as defined in Section 9.01 of the *Visa International Certificate of Incorporation and By-Laws* and the *Visa U.S.A. Inc. Certificate of Incorporation and By-Laws).*

- Redirecting Settlement funds to avoid potential losses, as specified in *Section X*, including, but not limited to, the following:

  – Rerouting Settlement funds around the financial institution that normally holds the Member's or agent's funds

  – Holding funds to ensure the correct application of Cardholder funds

  – Holding funds for the payment of Merchants

  – Holding funds for the future payment of Disputes

  – Withholding funds for the purpose of obtaining collateral or meeting other Member obligations

  – Prohibiting or limiting a Member's right to sponsor eligible Members

- Requiring a Member to change one or more of its designated agents

- Requiring a Member to provide to Visa data establishing, for any given time period, the amount of funds that a Merchant has received from Cardholders, for goods and services that it is yet to provide to those Cardholders

Visa is not obligated to take these actions to protect any Member, Merchant, Sponsored Merchant, or Cardholder from financial injury.

ID# 0005057   **Edition: Apr 2020 | Last Updated: Apr 2019**

1.10.1.3   Visa Right to Terminate Merchants, Payment Facilitators, Marketplaces, Sponsored Merchants, or Digital Wallet Operators

Visa may permanently prohibit a Merchant, Marketplace, Payment Facilitator, Sponsored Merchant, Digital Wallet Operator, or any other entity, or one or more of its principals, from participating in the Visa Program or Visa Electron Program for any reasons it deems appropriate, such as:

- Fraudulent activity

- Presenting Transaction Receipts that do not result from an act between a Cardholder and a Merchant or Sponsored Merchant (laundering)

- Entering into a Merchant Agreement or Payment Facilitator Agreement under a new name with the intent to circumvent the Visa Rules

- Activity that causes the Acquirer to repeatedly violate the Visa Rules

- Activity that has resulted in Visa prohibiting the Merchant, Sponsored Merchant, or Payment Facilitator from participating in the Visa Program or Visa Electron Program

- Exceeding the Visa Dispute Monitoring Program thresholds

- Entering illegal or brand-damaging Transaction activity into the Visa payment system
- Any other activity that may result in undue economic hardship or damage to the goodwill of the Visa system

Visa may contact a Merchant, a Marketplace and its retailers, a Sponsored Merchant, or a Payment Facilitator directly, if warranted.

In the Europe Region: An Acquirer may appeal to Visa with proof that the prohibition or any other conditions are impractical or unwarranted.

ID# 0007120	**Edition: Apr 2020 | Last Updated: Oct 2019**

1.10.1.4   Acquirer Responsibility for Costs Due to Failure to Terminate a Merchant

An Acquirer is responsible for all costs incurred by Visa due to the Acquirer's failure to terminate a Merchant, Marketplace, Sponsored Merchant, Payment Facilitator, or Staged Digital Wallet Operator. This includes attorney's fees and costs of any legal action undertaken by Visa to protect the goodwill of the Visa system or to prevent further harm to Members and Cardholders.

ID# 0007117	**Edition: Apr 2020 | Last Updated: Apr 2018**

1.10.1.5   Visa Anti-Bribery Program

Visa maintains an anti-bribery compliance program designed to comply with the requirements and restrictions of the *United States Foreign Corrupt Practices Act* and other anti-bribery laws. A Member must cooperate with Visa in the administration of the Visa anti-bribery program, including, but not limited to, the following:

- Complete, upon request, the *Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF), Sanctions and Anti-Bribery Compliance Program Questionnaire* disclosing the level of ownership, control, and influence of any non-US government, agency, or instrumentality thereof in the Member
- Notify Visa when a non-US government acquires (either as one agency or collectively through different agencies or instrumentalities) an equity interest of 30% or more in the Member

This does not apply in the US Region.

ID# 0008836	**Edition: Apr 2020 | Last Updated: Oct 2017**

1.10.1.6   Anti-Money Laundering Program Requirement

A Member must implement and maintain an anti-money laundering program that is reasonably designed to prevent the use of the Visa system to facilitate money laundering or the financing of terrorist activities.

ID# 0000652	Edition: Apr 2020 | Last Updated: Oct 2014

1.10.1.7   Visa Anti-Money Laundering Program – Member Requirements

A Member must cooperate with Visa in the administration of the Visa anti-money laundering program, including, but not limited to, the following:

- Completing the *Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF), Sanctions and Anti-Bribery Compliance Program Questionnaire* when requested by Visa and returning the form within the time limit specified by Visa
- Assisting Visa in guarding against Card issuance and Merchant acquiring in circumstances that could facilitate money laundering or the financing of terrorist activities
- Identifying circumstances of heightened risk and instituting policies, procedures, controls, or other actions specified by Visa to address the heightened risk
- Providing a copy of the Member's anti-money laundering plan if requested by Visa
- Ensuring the adequacy of the applicable controls implemented by designated agents of the Member

ID# 0000653	Edition: Apr 2020 | Last Updated: Oct 2017

1.10.1.8   Anti-Money Laundering Program Compliance

If Visa determines that a Member or the Member's designated agent has failed to comply with *Section 1.10.1.6, Anti-Money Laundering Program Requirement,* and *Section 1.10.1.7, Visa Anti-Money Laundering Program – Member Requirements,* Visa may impose conditions on or require additional actions of the Member or the Member's designated agent to prevent possible money laundering or financing of terrorist activities. These actions may include, but are not limited to, the following:

- Implementation of additional policies, procedures, or controls
- Termination of a Merchant Agreement
- Termination of a Cardholder agreement
- Termination of an agent agreement
- Termination of Visa membership
- Non-compliance assessments
- Other action that Visa in its sole discretion determines to take with respect to the Member or the Member's designated agent

ID# 0000654	Edition: Apr 2020 | Last Updated: Oct 2014

1.10.2   Brand Protection

1.10.2.1   Acquirer Brand Protection Requirements

An Acquirer must ensure that a Merchant, Marketplace, Payment Facilitator, Sponsored Merchant, or Staged Digital Wallet Operator does not accept Cards for, or display a Visa-Owned Mark on a website and/or an application that is used in relation to, either:

- The purchase or trade of photographs, video imagery, computer-generated images, cartoons, simulation, or any other media or activities including, but not limited to, activities listed in *Section 1.3.3.4, Brand Protection and Use of the Visa-Owned Marks*

- The purchase of products that claim or imply a similar efficacy as prescription drugs, controlled substances, or recreational/street drugs, irrespective of claims of legality

ID# 0026376   **Edition: Apr 2020 | Last Updated: Apr 2020**

1.10.2.2   Global Brand Protection Program – Requests for Information

An Acquirer must provide information relating to any request for information presented by Visa, its designees, or any regulatory agency, as required under the Global Brand Protection Program.

The Acquirer must provide the required information in writing as soon as possible, but no later than 7 business days following receipt of the request for information.

ID# 0026384   **Edition: Apr 2020 | Last Updated: Oct 2014**

1.10.3   Investigations

1.10.3.1   Investigation Assistance to Other Members

A Member must assist other Members in an investigation of fraudulent activity with a Card by performing tasks including, but not limited to, the following:

- Interviewing Merchants, Sponsored Merchants, Cardholders, suspects, witnesses, and law enforcement personnel

- Obtaining handwriting samples, photographs, fingerprints, and any other similar physical evidence

- Recovering lost, stolen, or Counterfeit Cards

- Providing information to proper authorities for the possible arrest of suspects, at the Issuer's request

- Performing any other reasonable investigative assistance

- Inspecting the facilities of credit card manufacturers, embossers, encoders, mailers, and chip embedders

ID# 0007122	Edition: Apr 2020 | Last Updated: Apr 2020

1.10.3.2   Investigation Assistance Standards – CEMEA and Europe Regions

In the CEMEA Region, Europe Region: A Member must respond to a request from another Member, Visa, or a law enforcement agency

ID# 0002249	Edition: Apr 2020 | Last Updated: Apr 2017

1.10.4   Information Security

1.10.4.1   Account and Transaction Information Security Requirements

A Member must:

- Maintain all materials or records in any form that contains account or Transaction Information in a safe and secure manner with access limited to authorized personnel, as specified in the *Payment Card Industry Data Security Standard (PCI DSS)*
- Ensure that agreements and contracts with agents and Merchants clearly establish their responsibilities to meet Visa standards, the liabilities for failure to meet the standards, and the requirement to allow for inspections by the Member or Visa
- Ensure that all agents and Merchants with access to account or Transaction Information comply with the *Payment Card Industry Data Security Standard (PCI DSS)*
- Ensure that all agents and Merchants do not store any of the following subsequent to Authorization:
  - Full contents of any data taken from the Magnetic Stripe (on a Card, in a Chip, or elsewhere)
  - Card Verification Value 2
  - PIN or the encrypted PIN block
  - Token Authentication Verification Value (TAVV)
  - Dynamic Token Verification Value (DTVV)
  - Visa Secure Cardholder Authentication Verification Value (CAVV)
- Comply with, and ensure that all agents and Merchants use Payment Applications that comply with, the *Payment Application Data Security Standard (PA-DSS)*

- Upon request, certify to Visa that agents and Merchants are in compliance with the *Payment Card Industry Data Security Standard (PCI DSS)*

- Comply with, and ensure that its Merchants, agents, and other third parties with access to account or Transaction Information comply with, the requirements of the Account Information Security Program. The Member must also ensure that its Merchants both:

  – Implement and maintain all Account Information Security Program requirements

  – If using a Third Party Agent, ensure that the Third Party Agent implements and maintains all of the security requirements specified in the Account Information Security Program

ID# 0002228	Edition: Apr 2020 | Last Updated: Oct 2019

1.10.4.2   Cardholder and Transaction Information Disclosure Limitations

An Acquirer must obtain the prior written consent of the Issuer and Visa before disclosing a Cardholder's Payment Credential, personal information, or other Transaction Information to a third party that is not the Agent of the Acquirer for the sole purpose of completing a Transaction. The Acquirer must ensure that its Agents and the Agents' employees both:

- Make no further disclosure of the information

- Treat the information as confidential

An Acquirer or Merchant may disclose Transaction Information to third parties without the prior consent of the Issuer and Visa only for the following:

- Supporting a loyalty program

- Providing fraud control services

- Assisting the Merchant in completing the initial Merchant Transaction

An Agent must not disclose a Payment Credential, Cardholder personal information, or other Transaction Information to third parties, other than for the sole purpose of completing the initial Merchant Transaction or with the permission of the Issuer, Acquirer, or Visa. Any such disclosure must be subject to strict, written, confidentiality obligations.

ID# 0026337	Edition: Apr 2020 | Last Updated: Apr 2020

1.10.4.3   Issuer Fraud Activity Reporting

A Member must immediately report all fraudulent activity or other criminal risk activity to Visa.

An Issuer must report[1] Fraud Activity through VisaNet, as specified in the *Fraud Reporting System (FRS) User's Guide*, when either a:

- Fraudulent user has obtained a Card or Payment Credential
- Card was obtained through misrepresentation of identification or financial status

The Issuer must report the Fraud Activity upon detection, but no later than:

- 60 calendar days from the Transaction Date
- 30 calendar days following the receipt of the Cardholder's dispute notification, if the notification is not received within the 60-calendar day period

At least 90% of rejected Fraud Activity must be resubmitted and accepted into the Fraud Reporting System.

In addition, for Intraregional Transactions in the Europe Region, an Issuer must report Fraud Activity through its Visa Scheme Processor, as follows:

- Upon detection, ensuring that 80% of fraud related to lost Cards, stolen Cards, Counterfeit Cards, and Cards not received is reported within 60 days of the Transaction Date, and the remaining 20% within 90 days
- Upon detection, ensuring that 65% of fraud related to fraudulent use of Payment Credentials is reported within 60 days of the Transaction Date and the remaining 35% within 90 days
- Immediately upon confirmation, but no later than 60 days after the Transaction Date

If an Issuer does not comply with these fraud reporting requirements, the Issuer is subject to non-compliance assessments.

[1] In the Europe Region: From the date a Payment Credential is reported to Visa, the Payment Credential is outside of the scope of the requirements of the Payment Card Industry Data Security Standard (PCI DSS) and Account Information Security Program.

ID# 0002389   Edition: Apr 2020 | Last Updated: Apr 2020

1.10.4.4   Counterfeit Activity Reporting

An Acquirer must report both:

- Counterfeit activity through VisaNet (or, in the Europe Region, through its Visa Scheme Processor), using the appropriate fraud advice transaction code in the same manner as specified for Issuers in _Section 1.10.4.3, Issuer Fraud Activity Reporting_
- A counterfeit Transaction within 60 calendar days of a Dispute, when no pre-Arbitration or Arbitration right is available

ID# 0002395   Edition: Apr 2020 | Last Updated: Oct 2019

1.10.5   High-Brand Risk Activity

1.10.5.1   High-Brand Risk Acquirer Requirements

Effective through 16 October 2020 An Acquirer of High-Brand Risk Merchants, High-Risk Internet Payment Facilitators, or High-Brand Risk Sponsored Merchants must do all of the following:

- Be investment-grade and have at least USD 100 million in equity capital[1]

- Comply with the Visa Rules and all requirements and policies

- Conduct appropriate due diligence to ensure compliance with the *Visa Global Acquirer Risk Standards*

- Be in good standing in all Visa risk management programs

- If required, complete and fully remediate an on-site operation review

Effective 17 October 2020 Before submitting Transactions completed by High-Brand Risk Merchants, High-Risk Internet Payment Facilitators, or High-Brand Risk Sponsored Merchants, an Acquirer must do all of the following:

- Submit to Visa a *High-Brand Risk Acquiring Registration Application* and be approved by Visa

- Be investment-grade and have at least USD 100 million in equity capital[1]

- Comply with the Visa Rules and all requirements and policies

- Conduct appropriate due diligence to ensure compliance with the *Visa Global Acquirer Risk Standards*

- Be in good standing in all Visa risk management programs

- If required, complete and fully remediate an on-site operational audit

- Register with Visa all of the following:

  – High-Brand Risk Merchants[2] (using the Program Request Management application)

  – High-Risk Internet Payment Facilitators and their High-Brand Risk Sponsored Merchants

  – Agents that solicit High-Brand Risk Merchants, as high-risk Agents or High-Risk Internet Payment Facilitators

[1] Visa may waive these requirements in exchange for assurance and evidence of the imposition of risk controls satisfactory to Visa. Such controls and requirements may include, but are not limited to, the pledging of additional collateral.

[2] In the US Region: This does not apply to Merchants assigned MCC 5122 or 5912 if the Merchant is accredited by the National Association of Boards of Pharmacy (NABP) or other regulatory body recognized by Visa.

ID# 0026383	Edition: Apr 2020 | Last Updated: Apr 2020

1.10.6   Recovered Cards

1.10.6.1   Recovered Card Return Requirement

An Acquirer must notify the Issuer, through Visa Resolve Online or an Electronic Documentation Transfer Method, that its Card has been recovered, as specified in _Section 10.7.2.1, Recovered Card Handling and Notification Requirements._

ID# 0001782   **Edition: Apr 2020 | Last Updated: Apr 2020**

1.10.7   Counterfeit Losses

1.10.7.1   Assignment of Liability for Counterfeit Transactions

Visa assigns liability to the Issuer or Acquirer for counterfeit Transactions, based on the following priorities in the order shown:

- The Acquirer, if the Merchant identified on a Visa Fraud Monitoring Program report in the enforcement period contributed to the origination of the Transaction Receipt[1] for a counterfeit Transaction

- The Acquirer first receiving the Transaction Receipt, if the BIN is not assigned to an Issuer

- The Acquirer that submitted the Transaction into Interchange, if an Authorization was required and not obtained or, where the Account Number is displayed on the Card, the Payment Credential encoded on the Magnetic Stripe of a Card was authorized but was different than the embossed or printed Account Number submitted into Interchange[1]

- The Issuer identified by the manufacturer product information printed on the reverse side of the Card, if the counterfeit Card was recovered and resulted from either the loss or theft of an unembossed and unencoded Card[1]

- The Issuer, if its BIN appears on the Transaction Receipt or Clearing Record for the counterfeit Transaction[1]

For a Transaction Receipt with an illegible or invalid Payment Credential, an Acquirer must comply with the applicable rules for counterfeit losses if it appears that a Transaction Receipt resulted from the use of either a:

- Counterfeit Card

- Misembossed or misencoded Card

In the Europe Region: There is no time limit on a Member's right to reassign liability to the Issuer for a Transaction in which a Counterfeit Card or a misencoded Card is used.

---

[1] For qualifying Transactions, the EMV liability shift, as specified in *Section 1.11.1.2, EMV Liability Shift Participation* takes precedence over this section to assess liability in the event of a conflict.

ID# 0001812	Edition: Apr 2020 | Last Updated: Apr 2020

1.10.8   Agents

1.10.8.1   VisaNet Processor and Visa Scheme Processor Registration

A Member that uses a VisaNet Processor, whether or not the VisaNet Processor is itself a Member, must submit to Visa a *VisaNet Processor and Third Party Registration and Designation (Exhibit 5E)* before using the VisaNet Processor.

A Member that uses a non-Member as a VisaNet Processor must ensure that the non-Member submits to Visa a *VisaNet Letter of Agreement (Exhibit 5A)* before using the non-Member as a VisaNet Processor.

In the Europe Region: In addition, a Member must do all of the following for a Processor or Visa Scheme Processor:

- Notify Visa of any change to the identity of the Processor or Visa Scheme Processor, or any change to the scope of the activities of the Processor or Visa Scheme Processor, within 5 business days of such change

- Only contract processing services to a Processor or Visa Scheme Processor that is compliant with the Payment Card Industry Data Security Standard (PCI DSS)

- Ensure that the Processor or Visa Scheme Processor (or third party) operates a separate funds transfer settlement reporting entity (FTSRE) for the transfer of the Settlement Amount

ID# 0025870	Edition: Apr 2020 | Last Updated: Oct 2016

1.10.8.2   Losses Resulting from Unauthorized Use

For losses resulting from Unauthorized Use, Visa may collect funds from one of the following, in the order listed:

- Member that caused the loss or Members using the Third Party Agent that caused the loss

- VisaNet Processor that processed the Transaction, if either:
  - No Member is directly responsible for the Unauthorized Use
  - The responsible Member does not meet its financial obligations

- Members using the VisaNet Processor, if the VisaNet Processor does not meet its financial obligations

---

ID# 0025888	Edition: Apr 2020 | Last Updated: Oct 2015

1.10.8.3   VisaNet Processor Contingency Plans

A Member must have in place contingency plans for its VisaNet Processors in the event of failure, including bankruptcy, insolvency, or other suspension of business operations. The contingency plans must be provided to Visa upon request.

ID# 0025877	Edition: Apr 2020 | Last Updated: Oct 2014

1.10.8.4   VisaNet Processor or Visa Scheme Processor Disclosure of Account or Transaction Information

A Member, in the event of the failure, including bankruptcy, insolvency, or other suspension of business operations of one of its VisaNet Processors or Visa Scheme Processors, must ensure that the VisaNet Processor or Visa Scheme Processor does not sell, transfer, or disclose any materials that contain Payment Credentials, personal information, or other Transaction Information to any other entity. The Member must ensure that its VisaNet Processor or Visa Scheme Processor either:

- Returns this information to the Member
- Provides acceptable proof of secure destruction of this information to the Member

ID# 0025875	Edition: Apr 2020 | Last Updated: Apr 2020

1.10.8.5   Third Party Agent Contract

A Third Party Agent must have a direct written contract with a Member to perform services on behalf of the Member.

ID# 0025892	Edition: Apr 2020 | Last Updated: Oct 2014

1.10.8.6   Third Party Agent Registration Requirements

A Member must register a Third Party Agent with Visa. The Member must both:

- Use the Program Request Management application
- Complete the appropriate regional forms

Registration must be completed before the performance of any contracted services or Transaction activity.

Visa may deny or reject a Third Party Agent's registration at any time with or without cause.

A Third Party Agent is exempt from the registration requirements and the associated fees if it only provides services on behalf of its affiliates (including parents and subsidiaries) that are Members that own and control at least 25% of the Third Party Agent.

ID# 0025893	Edition: Apr 2020 | Last Updated: Oct 2016

1.10.8.7   Merchant Third Party Agent Registration Requirements

An Acquirer must register with Visa a Third Party Agent that has been engaged by any of its Merchants before the performance of any contracted services by the Third Party Agent on behalf of the Merchant.

Registration of a Third Party Agent is specific to each Acquirer, and requires a separate registration by each Acquirer for any Third Party Agent that either:

- Uses its Acquiring Identifier
- Provides contracted services on behalf of the Acquirer or its Merchants

In the LAC Region: Registration is per Acquirer, per country, and per Third Party Agent.

ID# 0025894	Edition: Apr 2020 | Last Updated: Apr 2020

1.10.8.8   Assignment of Liability for Third Party Agents

If a Member fails to meet its responsibilities regarding Third Party Agents, Visa assigns liability in the following order of precedence:

- The Member from whose performance or nonperformance (including by its Third Party Agents) the loss arose
- The Member, if any, that sponsored the above Member, with limitations specified in the *Visa International Certificate of Incorporation and By-Laws*, Section 2.11
- BIN Licensees of BINs or Acquiring Identifier Licensees of Acquiring Identifiers used in Transactions, with limitations specified in *Section X*
- Other BIN Users or Acquiring Identifier Users, in an order determined by Visa

ID# 0025904	Edition: Apr 2020 | Last Updated: Oct 2019

1.10.9   Card Manufacturing and Distribution

1.10.9.1   Card Security Staff Requirements

An Issuer must have a qualified fraud control and Card security officer and staff that are primarily responsible for all areas of security for Cards. The security staff must do all of the following:

- Investigate all fraudulent use of the Issuer's Cards
- Plan and supervise the manufacturing, embossing, encoding, printing, and mailing of the Issuer's Cards
- Plan and supervise the physical protection of the Issuer's Center and building
- Participate in Center employee background investigations

ID# 0002394   **Edition: Apr 2020 | Last Updated: Apr 2020**

1.10.9.2   Visa Product Personalization

An Issuer that personalizes Visa Products on its own behalf must create and maintain a secure environment.

An Issuer that personalizes Visa Products on behalf of other Issuers must comply with all of the following:

- *Payment Card Industry (PCI) Card Production and Provisioning – Physical Security Requirements*
- *Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements*
- Applicable regional Issuer personalization policy

For each Third Party Agent performing Instant Card Personalization Issuance, the Issuer must validate the Third Party Agent's compliance with the *Visa Global Instant Card Personalization Issuance Security Standards*, and complete an annual self-audit against the *Visa Global Instant Card Personalization Issuance Security Standards,* for each location.

ID# 0025518   **Edition: Apr 2020 | Last Updated: Apr 2017**

1.10.9.3   Use of Approved Manufacturers, Approved Personalizers, and Approved Fulfillment Vendors

An Issuer that does not perform its own manufacturing, personalization, or fulfillment must do all of the following:

- Use a Visa-approved manufacturer to manufacture or print Visa Products[1]

- Ensure that the Visa-approved manufacturer is posted on the *Visa Global Registry of Service Providers*[2] and complies with the *Payment Card Industry (PCI) Card Production and Provisioning – Physical Security Requirements*

- Use a Visa-approved Card personalizer or Visa (if applicable) to personalize Visa Products, unless using an Instant Card Personalization Issuance Agent or another Issuer

- Ensure that the Visa-approved personalizer is posted on the *Visa Global Registry of Service Providers*[2]

- Use a Visa-approved fulfillment vendor to package, store, or ship Visa Products unless using a Distribution Channel Vendor for pre-manufactured, commercially ready Visa Products

- Ensure that the Visa-approved fulfillment vendor is posted on the *Visa Global Registry of Service Providers*[2]

- Immediately[3] notify Visa if the Visa-approved manufacturer, personalizer, and/or fulfillment vendor is unable to complete its responsibilities

- Contract through another Issuer, Visa (if applicable), or Visa-approved manufacturer, personalizer, or fulfillment vendor for the production, personalization, or fulfillment of Visa Products

- Review completed Card products for accuracy, including embossing, printing, and encoding

[1] In the Europe Region: An Issuer must ensure that its Cards (except Reference Cards) are produced by a Visa-approved manufacturer.

[2] In the Europe Region: An equivalent Visa list of approved service providers

[3] In the Europe Region: Within 5 days

ID# 0025517	Edition: Apr 2020 | Last Updated: Apr 2017

1.10.9.5   Use of Distribution Channel Vendors

An Issuer that uses a Distribution Channel Vendor must validate annually the Distribution Channel Vendor's compliance with the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors*.

ID# 0025520	Edition: Apr 2020 | Last Updated: Oct 2014

1.11   Dispute Resolution

1.11.1   Disputes

1.11.1.1   Attempt to Settle

Before initiating a Dispute, the Issuer must attempt to honor the Transaction.

If the attempt fails and the Issuer has already billed the Transaction to the Cardholder, the Issuer must credit the Cardholder for the disputed amount.

The Issuer must not be reimbursed twice for the same Transaction.

A Cardholder must not be credited twice as a result of both a Dispute and a Credit processed by a Merchant.

ID# 0003287	Edition: Apr 2020	Last Updated: Apr 2018

1.11.1.2   EMV Liability Shift Participation

The EMV liability shift applies to qualifying Transactions, as follows:

Table 1-10: EMV Liability Shift Participation

Region	Transactions in EMV Liability Shift
AP Region	All domestic,[1] intraregional, and interregional[2] counterfeit POS Transactions, except Domestic Transactions in Mainland China All domestic,[1] intraregional, and interregional[2] counterfeit ATM Transactions, except Indonesia,[3] and Domestic Transactions in Mainland China
Canada Region,[4] CEMEA Region,[4] Europe Region,[4] LAC Region[4]	All domestic, intraregional, and interregional[2] POS and ATM Transactions[5]
US Region	**Effective through 30 September 2020** All domestic and interregional[2] counterfeit POS and ATM Transactions, except Domestic Transactions at Automated Fuel Dispensers **Effective 1 October 2020** All domestic and interregional[2] counterfeit POS and ATM Transactions
[1] In the AP Region (Malaysia): Also includes fraudulent qualifying domestic non-counterfeit Transactions completed with a lost or stolen Card or "not received item" (NRI) except qualifying Visa Easy Payment Service Transactions	

Table 1-10: EMV Liability Shift Participation (continued)

Region	Transactions in EMV Liability Shift
[2] Among Visa Regions, individual countries and/or territories participating in the EMV liability shift	
[3] **Effective through 31 December 2021**	
[4] Except for fraudulent qualifying Visa Easy Payment Service Transactions completed with a lost or stolen Card or "not received item" (NRI)	
[5] Counterfeit, lost, stolen, and "not received item" (NRI) fraud only	

ID# 0008190	Edition: Apr 2020 | Last Updated: Apr 2019

1.11.2   Arbitration and Compliance

1.11.2.1   Invalid Arbitration or Compliance Case Rejection

If Visa determines that an Arbitration or Compliance request is invalid, it may reject the case and retain the review fee.

ID# 0001449	Edition: Apr 2020 | Last Updated: Apr 2020

1.11.2.2   Arbitration and Compliance Decision

Visa bases its Arbitration or Compliance decision on all information available to it at the time of reaching the decision, including, but not limited to, the provisions of the Visa Rules effective on the Transaction Date and may, at its sole discretion, consider other factors, such as the objective of ensuring fairness. The decision is delivered to both Members in writing and is final and not subject to any challenge, except for any right of appeal permitted in the Visa Rules.

ID# 0027133	Edition: Apr 2020 | Last Updated: Apr 2018

1.11.2.3   Arbitration or Compliance Financial Liability

An Arbitration or Compliance decision may result in either:

- One Member assigned full liability
- Members sharing financial liability

The responsible Member is financially liable for both:

- Transaction amount. For Arbitration cases, Visa will debit or credit the Members involved through Visa Resolve Online (VROL), as appropriate. For Compliance cases, if funds are not automatically transferred through VROL, the requesting Member may collect this amount from the opposing Member through VisaNet within 60 calendar days of the Notification date of the decision by the Arbitration and Compliance Committee.

- Review fee

When the case is adjudicated, Visa will collect the review fees through the Global Member Billing Solution from the responsible Member.

Either Member in an Arbitration or a Compliance case may also be liable for a non-compliance assessment for each technical violation of the applicable Visa Rules.

ID# 0003623	Edition: Apr 2020 | Last Updated: Apr 2020

1.11.2.4   Arbitration or Compliance Appeal

The decision on any permitted appeal of an Arbitration or Compliance ruling is final and not subject to any challenge.

ID# 0001440	Edition: Apr 2020 | Last Updated: Apr 2018

1.12   Fees and Non-Compliance Assessments

1.12.1   Fee Assessment by Visa

1.12.1.2   Fee Adjustments

If Visa confirms that a Member has either underpaid or overpaid its fees, Visa may process a fee adjustment. The fee adjustment time period is limited to the 2 years before the date that either of the following occurred:

- The overpayment or underpayment was reported to Visa by the Member.

- Visa discovered that an adjustment was due to the Member.

Visa reserves the right to collect an underpayment from a Member beyond the 2-year period.

Any collection or refund does not include interest.

ID# 0026403	Edition: Apr 2020 | Last Updated: Oct 2019

1.12.2   Non-Compliance Assessments

1.12.2.1   Visa Right to Impose Non-Compliance Assessments

The Visa Rules specify all of the following:

- Enforcement mechanisms that Visa may use for violations of the Visa Charter Documents or Visa Rules
- The procedure for the allegation and investigation of violations
- The rules and schedules for non-compliance assessments

A Member that does not comply with the Visa Charter Documents or Visa Rules will be subject to non-compliance assessments. Depending on the violation, a non-compliance assessment may be levied per Merchant, Merchant Outlet, Transaction, device, or Card, as defined by the impacted rule.

These procedures and non-compliance assessments are in addition to enforcement rights available to Visa under other provisions of the Visa Rules, or through other legal or administrative procedures.

Visa may assess, suspend, or waive non-compliance assessments, in whole or in part, to accommodate unique or extenuating circumstances.

Visa may, at its sole discretion, deviate from the schedules specified in *Section 1.12.2.2, General Non-Compliance Assessment Schedules,* and *Section 1.12.2.8, Willful or Significant Violations Schedules.* For example, this may be by using a different non-compliance amount entirely, or by additionally levying a non-compliance assessment from another schedule. In these instances, all of the following will be considered:

- Type of violation
- Nature of the damage, including the amount incurred by Visa and/or its Members
- Repetitive nature of the violation
- Member history or prior conduct
- Effect of the assessment upon the safety and soundness of the Visa system and the Member, including the Member committing the violation
- Any other criteria Visa deems appropriate

ID# 0007280   Edition: Apr 2020 | Last Updated: Oct 2019

1.12.2.2   General Non-Compliance Assessment Schedules

Effective through 24 January 2020 The non-compliance assessments specified in *Table 1-11, General Schedule of Non-Compliance Assessments,* may be assessed for a violation of the Visa Rules and are in addition to any other non-compliance assessments specified in the Visa Rules.

Effective through 24 January 2020 In the Europe Region: If a specific non-compliance assessment has been prescribed for the first violation only, the subsequent non-compliance assessments specified in *Table 1-11, General Schedule of Non-Compliance Assessments,* will apply for each repeated violation.

Table 1-11: General Schedule of Non-Compliance Assessments

Violation	Non-Compliance Assessment
First violation of rule	Warning letter with specific date for correction and USD 1,000 (in the Europe Region, USD 500)
Second violation of same rule in a 12-month period after Notification of first violation	USD 5,000
Third violation of same rule in a 12-month period after Notification of first violation	USD 10,000
Fourth violation of same rule in a 12-month period after Notification of first violation	USD 25,000
5 or more violations of same rule in a 12-month period after Notification of first violation	Visa discretion
If the 12-month period is not violation-free and the non-compliance assessments total USD 25,000 or more	Additional non-compliance assessment equal to all non-compliance assessments levied during that 12-month period

Effective 25 January 2020 Visa may assess a non-compliance assessment for a violation of the Visa Rules. Unless addressed by a specific non-compliance assessment program in *Chapter 12, Fees and Non-Compliance Assessments,* a violation to the Visa Rules is subject to either:

- For the rules contained in *Chapter 1, Visa Core Rules, Table 1-12, General Schedule of Non-Compliance Assessments – Tier 1*
- For all other Visa Rules, *Table 1-13, General Schedule of Non-Compliance Assessments – Tier 2*

Visa may, at its sole discretion, deviate from these schedules, for example by using a tier 2 non-compliance assessment for a core rule, as specified in *Section 1.12.2.1, Visa Right to Impose Non-Compliance Assessments.*

Visa Core Rules and Visa Product and Service Rules

Where the violation is considered "willful" or "significant," non-compliance assessments in *Section 1.12.2.8, Willful or Significant Violations Schedules,* may also be applied.

Table 1-12: General Schedule of Non-Compliance Assessments – Tier 1

Event	Visa Action/Non-Compliance Assessment
Notification issued for violation of a rule	Warning letter with a request for a compliance/resolution plan
Response date has passed and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 25,000
30 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 50,000
60 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 75,000
90 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 150,000 Non-compliance assessments will continue to be levied each month until the rule violation is corrected, with the amount doubling each month.

Table 1-13: General Schedule of Non-Compliance Assessments – Tier 2

Event	Visa Action/Non-Compliance Assessment
Notification issued for violation of a rule	Warning letter with a request for a compliance/resolution plan

Table 1-13: General Schedule of Non-Compliance Assessments – Tier 2 (continued)

Event	Visa Action/Non-Compliance Assessment
Response date has passed and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 5,000
30 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 10,000
60 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 25,000
90 calendar days have passed after response due and either: • Rule violation not corrected • Rule violation corrected but violation of same rule repeated after correction	Non-compliance assessment of USD 50,000 Non-compliance assessments will continue to be levied each month until the rule violation is corrected, with the amount doubling each month.

ID# 0000482   **Edition: Apr 2020 | Last Updated: Oct 2019**

1.12.2.3   Determination of Violation of the Visa Rules

Determination of a violation of the Visa Charter Documents or Visa Rules may be made based on one of the following:

• The response from a Member to a Notification of investigation and other available information. Visa will determine whether a violation of the Visa Charter Documents or Visa Rules has occurred.

• A review by Visa of the evidence in relation to the identified violation, including any previous compliance cases and/or audit findings.

- The Member's failure to respond to a Notification of investigation and to provide all information requested.

ID# 0001052	Edition: Apr 2020 | Last Updated: Oct 2019

1.12.2.4   Notification of Determination of Violation

Visa will notify a Member if it determines that a violation of the Visa Charter Documents or Visa Rules has occurred, or if it determines that a violation is continuing to occur, and will specify a date by which the Member must correct the violation. The Notification will advise the Member of all of the following:

- Reasons for such determination

- Non-compliance assessment amount

- Right to appeal the determination and/or the non-compliance assessments for the violation, as specified in *Section 1.12.2.9, Enforcement Appeals*

Visa may require a Member to submit a compliance plan to resolve the violation.

ID# 0001053	Edition: Apr 2020 | Last Updated: Oct 2019

1.12.2.5   Non-Compliance Assessment Member Responsibility

A non-compliance assessment is imposed by Visa on a Member. A Member is responsible for paying all non-compliance assessments, regardless of whether it absorbs them, passes them on, or increases them in billing its customer (for example: Cardholder or Merchant). A Member must not represent to its customer that Visa imposes any non-compliance assessment on its customer.

ID# 0001054	Edition: Apr 2020 | Last Updated: Oct 2019

1.12.2.8   Willful or Significant Violations Schedules

Effective through 24 January 2020 In addition to the non-compliance assessments specified in the Visa Rules, a Member found to have willfully violated the Visa Rules, adversely affecting the goodwill associated with the Visa system, brand, products and services, operation of the Visa Systems, or operations of other Members will be subject to a further non-compliance assessment. A violation is considered "willful" if the Member knew, or should have known, or its knowledge can be fairly implied, that its conduct constituted a violation of the Visa Rules.

Effective through 24 January 2020 When determining the amount of a non-compliance assessment, in addition to the criteria above, all of the following will be considered:

- Type of violation

- Nature of the damage, including the amount incurred by Visa and its Members

- Repetitive nature of the violation

- Member history or prior conduct

- Effect of the assessment upon the safety and soundness of the Visa system and the Member, including the Member committing the violation

- Any other criteria Visa deems appropriate

Effective 25 January 2020 A Member found to have either willfully and/or significantly violated the Visa Rules, adversely affecting the goodwill associated with the Visa system, brand, products and services, operation of the Visa systems, or operations of other Members, will be subject to a non-compliance assessment for either:

- Violations as specified in *Table 1-14, Non-Compliance Assessments for Willful Violations of the Visa Rules,* where a violation is considered "willful" in that the Member knew, or should have known, or its knowledge can be fairly implied, that its conduct constituted a violation of the Visa Rules

- Violations as specified in *Table 1-15, Non-Compliance Assessments for Significant Violations of the Visa Rules,* where a violation is considered "significant" in that the Member's action, error or omission, intended or unintended, known or unknown, presents immediate and/or substantial risks, economic or otherwise, to Visa, its Members, Cardholders, Merchants, and/or a country's applicable laws or regulations

Effective 25 January 2020 Visa may, at its sole discretion, deviate from these schedules, as specified in *Section 1.12.2.1, Visa Right to Impose Non-Compliance Assessments.*

Table 1-14: Non-Compliance Assessments for Willful Violations of the Visa Rules

Event	Visa Action/Non-Compliance Assessment
Notification issued for violation of a rule	Both: - Warning letter with a request for a compliance/resolution plan - USD 50,000 non-compliance assessment (payment will be suspended until end date for correction)
Response date has passed and either: - Rule violation not corrected - Rule violation corrected but violation of same rule repeated after correction within a 12-month	Non-compliance assessment, between USD 100,000 and USD 1,000,000 Non-compliance assessments will continue to be levied each month in increasing amounts, at Visa

Table 1-14: Non-Compliance Assessments for Willful Violations of the Visa Rules (continued)

Event	Visa Action/Non-Compliance Assessment
period	discretion, until the rule violation is corrected.

Table 1-15: Non-Compliance Assessments for Significant Violations of the Visa Rules

Event	Visa Action/Non-Compliance Assessment
Notification issued for violation of a rule	Both: - Warning letter with a request for a compliance/resolution plan - USD 50,000 non-compliance assessment (payment will be suspended until end date for correction)
Response date has passed and either: - Rule violation not corrected - Rule violation corrected but violation of same rule repeated after correction within a 12-month period	Non-compliance assessment, between USD 50,000 and USD 500,000 Non-compliance assessments will continue to be levied each month in increasing amounts, at Visa discretion, until the rule violation is corrected.

ID# 0007288   **Edition: Apr 2020 | Last Updated: Oct 2019**

1.12.2.9   Enforcement Appeals

A Member may appeal a determination of a violation or non-compliance assessment to Visa where the Member can provide new evidence not previously available that shows a violation did not occur, as follows:

- The Member's appeal letter must be received by Visa within 30 calendar days of the Member's receipt of the Notification of the violation or non-compliance assessment.

- The appealing Member must submit with the appeal any new or additional information or supporting arguments necessary to substantiate its request for an appeal.

- A fee of USD 5,000 will be assessed to the Member upon receipt of the appeal. This fee is refundable if the appeal is upheld.

Visa will make its decision. All decisions are final and not subject to challenge.

ID# 0025975   **Edition: Apr 2020 | Last Updated: Oct 2019**

Part 2:
Visa Product and Service Rules

2   Licensing and Numerics Management

2.1   Membership

2.1.1   Member Acquisitions and Mergers

2.1.1.1   Member Acquisition upon Regulatory Closure – US Region

In the US Region: In the event of a regulatory closure, the assuming organization must comply with the requirements specified in *Table 2-1, Regulatory Closure – Assuming Member Requirements.*

Table 2-1: Regulatory Closure – Assuming Member Requirements

Condition	Required Action
Assuming organization is not a Member at the time of its assumption of Visa programs and is eligible for membership	• Submit to Visa a *Client Licensing Application* agreement within 10 calendar days after the assuming organization's assumption of the Visa programs • Submit the appropriate membership materials within the time specified by Visa • Meet any conditions of membership within 30 calendar days of the assuming organization's assumption of the Visa programs
Assuming organization is not a Member at the time of its assumption of Visa programs and does not submit the required *Client Licensing Application* agreement within the specified time	• Cease all operations of the Visa programs and use of the Visa-Owned Marks • Be liable for Liabilities asserted against or incurred by Visa and its Members resulting from unauthorized operations
Assuming organization is not a Member of Visa at the time of its assumption of Visa programs and is not eligible for the appropriate membership or if Visa declines its application	Immediately cease both: • All use of the Visa-Owned Marks and all other activities reserved for Members • Exercising the rights and privileges reserved for Members
Assuming Member is not authorized to engage in one or more of the assumed Visa programs	• Submit the appropriate membership materials within the time frame specified by

Table 2-1: Regulatory Closure – Assuming Member Requirements (continued)

Condition	Required Action
	Visa ● Meet any conditions of membership within 30 calendar days of the Assuming Member's assumption of the Visa programs

A Member that assumes the Visa programs of a failed Member immediately assumes full liability for those Visa programs.

Upon verification from the applicable regulatory agency that a Member has assumed the Visa programs of a failed Member, Visa will provide Notification listing the Visa programs for which Visa understands the Assuming Member is liable.

The Assuming Member must submit to Visa, within the time specified in the Notification, written confirmation of the Visa programs assumed.

ID# 0025752	Edition: Apr 2020	Last Updated: Apr 2018

2.1.1.5   Termination of Membership – LAC Region (Brazil)

In the LAC Region (Brazil): A membership status may be terminated either:

● As a result of the client's substantial non-compliance with the business plan or description presented to, or agreed with Visa do Brasil as a condition for its participation in the Visa payment system

● If the client has no reported sales volume for a minimum of one year

ID# 0029264	Edition: Apr 2020	Last Updated: Apr 2018

2.1.2   Acquirer Licensing

2.1.2.1   Acquirer Licensing Requirements – LAC Region (Brazil)

In the LAC Region (Brazil): A Member must obtain a Merchant acquiring license before performing any acquiring activities within its jurisdiction, even if the Member already holds a Principal-type or an Associate-type license.

ID# 0027804	Edition: Apr 2020	Last Updated: Oct 2014

2.1.4   Changes to Member Information or Status

2.1.4.2   Client Directory Data Submission

A Member that is assigned a BIN or Acquiring Identifier must submit any new or revised information in the Visa Client Service Provider Directory module of the Client Directory via Visa Online, as follows:

- All directory data: Within 10 business days of a BIN or an Acquiring Identifier implementation
- All directory updates: Within 10 business days of the effective date of the change

A Member that is assigned a BID must submit any new or updated contact information, including the designation of a primary center manager contact, for its organization in the Client Contact Tool module of the Client Directory, as follows:

- Contact data: Within 10 business days of a BID implementation
- Contact updates: Within 10 business days of the effective date of the change

ID# 0007725   **Edition: Apr 2020 | Last Updated: Oct 2019**

2.3   BIN and Acquiring Identifier License and Administration

2.3.1   BIN and Acquiring Identifier Use and License

2.3.1.1   Sponsor and Licensee Responsibilities for BINs and Acquiring Identifiers

A Principal-Type Member must license and use only its assigned BIN or Acquiring Identifier.

An Associate-Type Member must either:

- License its own BIN or Acquiring Identifier. A BIN or an Acquiring Identifier licensed to an Associate-Type Member on or after 22 July 2017 must have only one Sponsor.
- Use a BIN or an Acquiring Identifier licensed to its sponsoring Principal-Type Member. The Principal-Type Member must ensure that the BIN or Acquiring Identifier is unique to the Associate-Type Member.

A Participant-Type Member does not have the right to license a BIN or an Acquiring Identifier, and must use only a BIN or an Acquiring Identifier designated to it by its Sponsor in accordance with the applicable Visa Charter Documents.

A BIN or an Acquiring Identifier may have only one BIN Licensee or Acquiring Identifier Licensee. The BIN Licensee is responsible[1] for all activities associated with any BIN that it licenses. The

Acquiring Identifier Licensee is responsible for all activities associated with any Acquiring Identifier that it licenses.

A Sponsor's responsibility is limited to the BINs or Acquiring Identifiers associated with the sponsoring relationship between the Sponsor and the Sponsored Member.

If a BIN User or an Acquiring Identifier User is no longer authorized by the BIN Licensee or Acquiring Identifier Licensee to use its BIN or Acquiring Identifier, the BIN User or Acquiring Identifier User must discontinue use of the BIN or Acquiring Identifier.

A BIN Licensee or an Acquiring Identifier Licensee, or its designated Sponsored Member, must use a BIN or an Acquiring Identifier Licensee only for a purpose approved by Visa, or Visa may block and remove the BIN or Acquiring Identifier from VisaNet.

A BIN Licensee and an Acquiring Identifier Licensee must do all of the following:

- Maintain the accuracy of the information relative to the BIN or Acquiring Identifier
- Notify Visa of any inaccuracies on BIN or Acquiring Identifier licensing reports
- Notify Visa of, or request, any changes to the BIN or Acquiring Identifier

Responsibility for activities associated with a Token is assigned to the BIN Licensee for the Account Number represented by the Token.

[1] This does not apply to a BIN licensed to Visa for the provision of Tokens to Issuers.

ID# 0001225	Edition: Apr 2020	Last Updated: Apr 2020

2.3.1.2   VisaNet Processor BIN and Acquiring Identifier Use

A Member that designates a VisaNet Processor or Visa Scheme Processor to act on its behalf must ensure that the VisaNet Processor or Visa Scheme Processor only:

- Processes transactions on the Member's BIN(s) or Acquiring Identifier(s) for activities for which the BIN or Acquiring Identifier is licensed
- Processes transactions on the Member's BIN(s) or Acquiring Identifier(s) that are originated by the BIN Licensee or Acquiring Identifier Licensee or the BIN Licensee's or Acquiring Identifier Licensee's Sponsored Members approved to share the BIN or Acquiring Identifier
- Clears or settles transactions on the Member's BIN(s) or Acquiring Identifier(s) that are originated by the BIN Licensee or Acquiring Identifier Licensee or the BIN Licensee's or Acquiring Identifier Licensee's Sponsored Members approved to share the BIN or Acquiring Identifier

A VisaNet Processor or Visa Scheme Processor that is not also a Member must both:

- Use its licensed BINs or Acquiring Identifiers exclusively for processing activities

- Not use the BINs for issuing purposes or Acquiring Identifiers for acquiring purposes

ID# 0001227	Edition: Apr 2020 | Last Updated: Oct 2019

2.3.1.3   BIN and Acquiring Identifier Conversion to Newly Designated VisaNet Processor or Visa Scheme Processor

If a Member converts a BIN or an Acquiring Identifier to a newly designated VisaNet Processor or Visa Scheme Processor, the Member must require the new VisaNet Processor or Visa Scheme Processor to complete any activity associated with the converted BIN or Acquiring Identifier.

This does not apply if the former VisaNet Processor or Visa Scheme Processor agrees to complete the activity associated with the converted BIN or Acquiring Identifier.

ID# 0001269	Edition: Apr 2020 | Last Updated: Oct 2019

2.3.1.4   Sponsor Liability – AP, CEMEA, LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Principal-Type Member is responsible and liable for all activities, including accuracy of information provided to or received from Visa, for BINs or Acquiring Identifiers licensed directly to an Associate-Type Member that it sponsors. The Sponsor's liability is limited to the BINs or Acquiring Identifiers associated with the sponsorship relationship between the Principal-Type Member and Associate-Type Member.

ID# 0026466	Edition: Apr 2020 | Last Updated: Oct 2019

2.3.1.5   BIN Currency – Europe Region

In the Europe Region: An Issuer must ensure that the denominated currency of the BIN on which a Card is issued is the same as the Billing Currency.

ID# 0029568	Edition: Apr 2020 | Last Updated: Oct 2019

2.3.2   Administration of BINs, Acquiring Identifiers, and Numerics

2.3.2.1   Release of BINs and Acquiring Identifiers

A BIN Licensee or an Acquiring Identifier Licensee that no longer uses a BIN or an Acquiring Identifier must release it to Visa.

When a BIN Licensee or an Acquiring Identifier Licensee releases a BIN or an Acquiring Identifier to Visa, all of the following apply:

- The BIN Licensee or Acquiring Identifier Licensee remains liable for any exception activity and fees related to the BIN or Acquiring Identifier that were incurred prior to its release.

- The BIN Licensee or Acquiring Identifier Licensee must notify all impacted parties that they must delete the released BIN or Acquiring Identifier from their systems. Visa reserves the right to notify, and provide relevant documentation to, impacted parties.

- Voluntary termination of membership will not be effective until all BINs, Acquiring Identifiers, and other Numeric IDs assigned to the Member are released from the Member's assignment.

- The BIN or Acquiring Identifier must have been inactive for at least 120 days. Visa will determine the eligible date of the BIN release from its current assignment based on the last date of approving authorizations or, for the Acquiring Identifier release from its current assignment, based on the last date of acquiring activity.

ID# 0001272	Edition: Apr 2020	Last Updated: Oct 2019

2.3.2.2 Private Label BIN Use

If a BIN Licensee or its designated Sponsored Member uses a BIN for a Private Label Card program, the Issuer or its Sponsored Member must have a written acceptance agreement directly with each Merchant that accepts its Private Label Cards.

ID# 0001253	Edition: Apr 2020	Last Updated: Oct 2019

2.3.2.3 Use of BINs and Acquiring Identifiers for Non-Visa Programs

In the AP Region, Canada Region, CEMEA Region, Europe Region (non-EEA countries only), LAC Region, US Region: A BIN or an Acquiring Identifier must not be used in connection with any non-Visa program, payment network, or system, including any non-Visa program that is co-badged or co-resident with a Visa Program, without written approval from Visa. If a Member receives Visa permission to use a BIN or Acquiring Identifier for a non-Visa program (including, but not limited to, a Private Label Card program), it must use the BIN or Acquiring Identifier only for the approved non-Visa program.

In the Europe Region (EEA countries only): A Member must notify Visa in advance if the Member intends to use a BIN or Acquiring Identifier for non-Visa purposes. The Member must use the BIN or Acquiring Identifier only as specified in the notification to Visa.

ID# 0001228	Edition: Apr 2020	Last Updated: Oct 2019

2.3.2.4   Use of Numeric ID

A Member, VisaNet Processor, or Visa Scheme Processor that receives a Numeric ID must ensure that the Numeric ID is used only for the activity approved by Visa.

A licensee of a Numeric ID is responsible for all of the following:

- Notifying Visa of any changes to the Numeric ID, including:
  - Portfolio sale or transfer
  - Merger or Acquisition
  - Cessation of use
  - Modification to service
  - Change in user
- All fees for the assignment and administration of the Numeric ID
- Compliance with *Section 2.3.2.1, Release of BINs and Acquiring Identifiers,* for alternate routing identifiers, as applicable
- All activity occurring on the Numeric ID until it is fully deleted from VisaNet

If a Numeric ID is used for a purpose other than that approved by Visa, Visa may block and remove the Numeric ID from VisaNet.

ID# 0026469   Edition: Apr 2020 | Last Updated: Oct 2019

2.3.3   Account Range and BIN Use

2.3.3.1   Combining Card Programs on a Single BIN

An Issuer must not combine the following on a single BIN:[1]

- Credit Cards, Debit Cards, and Prepaid Cards
- Visa Consumer Cards and Visa Commercial Cards

[1] In the LAC Region (Brazil): This does not apply for Visa Agro Cards.

ID# 0003144   Edition: Apr 2020 | Last Updated: Apr 2020

2.3.4 Use and Disclosure of BIN Information

2.3.4.1 Disclosure of BIN Attributes

BIN Attributes are proprietary and must not be disclosed to Merchants or any other party, except as follows:

- To a Member's Agent,[1] to the extent necessary to conduct the operational activities required to process Transactions

- To the extent that disclosure is required for a Member, a Merchant, or a Member's or Merchant's agent to comply with applicable laws or regulations

- In the AP Region (Australia), Canada Region, Europe Region (European Economic Area [EEA] countries only), US Region, US Territory: To identify Visa product types at the POS, if a Merchant implements limited acceptance. An Acquirer must provide BIN Attributes to any Merchant requesting them for this purpose.

- For any other reason, only if registered to share BIN Attributes and with prior written approval from Visa

If a Member or its agent provides BIN Attributes to a Merchant or any other party[1] for permitted purposes, it must do all of the following:

- Include terms expressly restricting permission for BIN Attributes to be used only for the permitted purpose in its Merchant Agreement or Agent contract, as applicable

- Provide updated BIN Attributes to the Merchant or other party as soon as reasonably possible after receipt

- Ensure that the Merchant or other party uses the updated BIN Attributes provided to it by the Member

An entity that receives BIN Attributes must both:

- Not disclose BIN Attributes to any Merchant or other party without prior written approval from Visa and treats BIN Attributes as proprietary and confidential information belonging to Visa and with the same degree of care as information labeled "Visa Confidential"

- Use BIN Attributes only as permitted in writing by Visa

[1] In the Europe Region: An Acquirer must not share BIN Attributes for Non-Reloadable Prepaid Cards with Merchants or Third Party Agents, as specified in *Section 5.9.1.16, Acquirer Use of Non-Reloadable Prepaid BIN and Account Range Data – Europe Region*.

ID# 0028285 Edition: Apr 2020 | Last Updated: Apr 2020

2.4   Marks License

2.4.1   Marks License Grant

2.4.1.1   License Grant for Visa-Owned Marks

Visa grants to each Member a non-exclusive, non-transferable license[1] to use each of the Visa-Owned Marks, including Interlink and Plus, only in conjunction with the applicable Visa Programs that are licensed to the Member.

[1] In the Europe Region: And royalty-free

ID# 0008906	Edition: Apr 2020	Last Updated: Apr 2018

2.4.1.2   License for Plus Card Acceptance – US Region

In the US Region: Visa grants a Member that is required to display the Plus Symbol on its ATM a license to use each of the Plus Program Marks for the purpose of accepting Plus Cards at ATMs, subject to the *Plus System, Inc. Bylaws and Operating Regulations*. A Member granted such a license acknowledges that Visa owns the Plus Program Marks.

ID# 0007436	Edition: Apr 2020	Last Updated: Oct 2014

2.5   Visa US Regulation II Certification Program

2.5.1   Visa US Regulation II Certification Program – US Region and US Territories

2.5.1.1   Visa US Regulation II Certification Program Requirements – US Region and US Territories

In the US Region or a US Territory: A BIN Licensee that is subject to US Federal Reserve Board Regulation II must comply with the Visa US Regulation II Certification Program requirements.

The BIN Licensee is solely responsible for ensuring that all consumer debit, commercial debit, and prepaid programs conducted under its BINs comply with applicable laws or regulations, including US Federal Reserve Board Regulation II.

The BIN Licensee or proposed BIN Licensee must submit a *Dodd-Frank Act Certification Addendum* and *Fraud Prevention Adjustment Addendum*, as applicable, when requesting, modifying, or transferring a consumer debit, commercial debit, or prepaid BIN.

An Issuer that is subject to US Federal Reserve Board Regulation II and that receives certification materials from Visa is required to respond within the published timeframes.

Any Issuer of consumer debit, commercial debit, or prepaid programs that is subject to the US Federal Reserve Board Regulation II and that receives fraud-prevention standards notification materials from Visa is required to respond within the published timeframes.

An Issuer subject to US Federal Reserve Board Regulation II must submit the notification materials, as applicable, if the Issuer's compliance with the fraud prevention standards has changed.

ID# 0027000	Edition: Apr 2020 | Last Updated: Oct 2014

2.6   Product-Specific BIN Requirements

2.6.1   Visa Consumer Products

2.6.1.1   Visa Health Savings Account (HSA) BIN Requirements – US Region

In the US Region: An Issuer must use a unique consumer Prepaid Card BIN designated for Health Savings Account (HSA) programs to issue HSA Cards.

The Issuer may use an existing Debit Card BIN if the HSA program complies with all of the following:

- Does not use Third Party Agents
- Has no restrictions on MCC or ATM access
- Will have less than 10,000 accounts issued

ID# 0025544	Edition: Apr 2020 | Last Updated: Apr 2020

2.7   Client Portfolio Management Self-Service Tools

2.7.1   Client Portfolio Management Self-Service Tools Requirements

2.7.1.1   Client Portfolio Management Self-Service Tools Information

A Member, VisaNet Processor, or designated Agent must not disclose any information from the Client Portfolio Management Self-Service Tools, or any other information associated with the tools, to any other parties unless it is permitted in the Visa Rules or otherwise authorized in writing by Visa. Information from and associated with the Client Portfolio Management Self-Service Tools is

the property of Visa and is for the sole use of Visa Members and their registered third-party service providers in support of the Members' Visa programs.

ID# 0026518	Edition: Apr 2020 | Last Updated: Oct 2014

2.7.1.2   Use of Client Portfolio Management Self-Service Tools

A Member is responsible for all of the following for a Member, VisaNet Processor, or designated Agent that has been granted permission to access the Client Portfolio Management Self-Service Tools on the Member's behalf:

- The Member's use and its VisaNet Processor's or designated Agent's use in accordance with the Visa Rules

- Monitoring its users' access to ensure that only authorized users are granted access to the service

- Ensuring that only authorized officers of the institution approve membership requests

- The accuracy of all information and any changes made to the information by the Member and its authorized users

- Ensuring that changes to the Member's information are accompanied by an Electronic Signature

ID# 0026519	Edition: Apr 2020 | Last Updated: Oct 2014

2.8   Non-Visa BINs and Acquiring Identifiers

2.8.1   Non-Visa-Assigned BINs and Acquiring Identifiers

2.8.1.1   Management of Non-Visa-Assigned BINs and Acquiring Identifiers

A BIN Licensee or an Acquiring Identifier Licensee of a non-Visa-assigned BIN or Acquiring Identifier that is used for a Visa service must both:

- Maintain the accuracy of the information relative to the BIN or Acquiring Identifier

- Notify Visa of any changes to the BIN or Acquiring Identifier, including any release of the BIN or Acquiring Identifier from its approved use

A BIN Licensee of a non-Visa-assigned BIN and an Acquiring Identifier Licensee of a non-Visa-assigned Acquiring Identifier must comply with *Section 2.3, BIN and Acquiring Identifier License and Administration.*

ID# 0026514	Edition: Apr 2020 | Last Updated: Oct 2019

2.10   EU Passporting

2.10.1   EU Passporting – Europe Region

2.10.1.1   Host Country Activity – European Economic Area

Where a Member located in the European Economic Area (EEA) chooses to operate outside of its home country and provide services in one or more host countries across the EEA, it must provide to Visa written confirmation that that Member has all necessary regulatory permissions for the provision of those services.

Where a Member operates in one or more host countries, it must do all of the following:

- For issuing activity, distinguish between Cards issued in a Home Country and a Host Country by allocating and using one or more unique BIN(s), or Account Ranges within a BIN, to identify each country in which issuance takes place
- Settle in a Visa-approved Settlement Currency for any given host country
- Participate in the respective National Net Settlement Service (NNSS), where applicable

An Acquirer that has passported its license into one or more Host Countries may allocate the same Acquiring Identifier for acquiring activity in its Home Country and Host Countries.

ID# 0029790   **Edition: Apr 2020 | Last Updated: Apr 2020**

3   Use of Marks

3.1   Marks License

3.1.1   Affinity/Co-Branded Card Programs

3.1.1.1   Affinity/Co-Branded Card Marks Prohibitions

An Affinity/Co-Branded Card must not bear:

- A Mark or name similar to an existing Visa program or service

- A Mark or image that is political, provocative, or socially offensive, as determined by Visa, that would result in non-acceptance of the Card or other issues at the Point-of-Transaction

- A Functional Type or Mark that facilitates payment for goods or services

ID# 0027368	Edition: Apr 2020 | Last Updated: Apr 2017

3.1.1.2   Affinity/Co-Brand Program Positioning and Advertising

An Affinity/Co-Brand Card Issuer must comply with all of the following:

- Position the Card as a Visa Card[1]

- Refer to the Affinity/Co-Brand Card as a "Visa Card" in all Collateral Material

- Ensure that all Collateral Material and Cards clearly state that the Member is the Issuer of the Card

- Ensure that the Visa Brand Name or Visa Brand Mark is prominently featured, or is at least the same size as, Marks owned by the Issuer and the Affinity/Co-Brand partner on all Collateral Material

- Not position the Card as adding superior acceptability at the Point-of-Transaction[2]

- Not state or imply that the Affinity/Co-Brand Card is accepted only by a particular Merchant or class of Merchants

- Portray itself as the owner of the Affinity/Co-Brand program

- Ensure that the Affinity/Co-Brand partner does not state or imply that the Affinity/Co-Branded Card is owned or issued by the Affinity/Co-Brand partner

Visa may prohibit the use of any materials that denigrate the Visa brand.

[1] In the US Region: A limited exception is allowed for Campus Cards to facilitate closed-loop proprietary college or

university system transactions and permit the use of campus identification/access applications. A Campus Card must still be positioned as a Visa Card, but with the additional functionality noted here.

2 This requirement does not apply to discounts, offers, or in-kind incentives offered by the Merchant.

ID# 0027369	Edition: Apr 2020 | Last Updated: Oct 2015

3.1.2   Marks License Grant

3.1.2.1   Registration/Ownership Denotation

A Member desiring to use a denotation or legend of registration or ownership with any proprietary Mark or Trade Name used in association with, or on the same piece as, any Visa-Owned Mark may do so only if proper trademark attribution is given to the Visa-Owned Mark as follows:

[Visa-Owned Mark] is a trademark owned by Visa International Service Association and used under license.

ID# 0007431	Edition: Apr 2020 | Last Updated: Oct 2014

3.1.3   Sponsorships and Partnerships, Including the Olympics

3.1.3.1   Marketing Partnership/Sponsorship Agreement

A partnership or sponsorship agreement governs in the case of ambiguity, conflict, or inconsistency between that agreement and the Visa Rules or any contract, sublicense, agreement, or other arrangements between Visa and a Member, a Merchant, or an affiliate.

ID# 0001128	Edition: Apr 2020 | Last Updated: Oct 2014

3.1.3.2   Sponsorship/Member Use of Marks

A Member's enjoyment of pass-through rights to use the Marks and promotional materials of any organization with which Visa has signed a global sponsorship agreement is always subject to the prior written approval of Visa and the partner or sponsor organization.

A Member must not use the Visa-Owned Marks with the Marks of any of the following, or of its subsidiaries or affiliates, in any sponsorship activity:

- American Express Company
- Discover Financial Services

- MasterCard Worldwide (including Maestro)
- Any other entity that Visa deems competitive

Upon Notification from Visa, a Member must correct any improper use of the partnership or Sponsorship Marks.

ID# 0007450	Edition: Apr 2020 | Last Updated: Oct 2014

3.1.3.3   Member as Sponsor

A Member that participates in any sponsorship activity of which Visa is the sponsor must clearly convey in all of its communications and displays that only Visa, not the Member, is the sponsor.

A Member that participates in any sponsorship activity of which the Member is granted sponsorship rights by Visa must clearly convey in all of its communications and displays that only the Member, not Visa, is the sponsor. The Member must not state or imply that it owns any of the Visa-Owned Marks.

ID# 0007405	Edition: Apr 2020 | Last Updated: Oct 2014

3.2   Use of Marks

3.2.1   Use of Marks by Members and Merchants

3.2.1.1   Use of Visa-Owned Marks

A Member or Merchant that uses a Visa-Owned Mark must comply with all of the following:

- Not use the Visa-Owned Mark in a way that implies endorsement of any other product or service
- Not use, adopt, register, or attempt to register a company name, product name, or Mark that is confusingly similar to any Visa product or service name or any Visa-Owned Mark
- Ensure that any material on which the Visa-Owned Mark appears does not infringe, dilute, or denigrate any of the Visa-Owned Marks or Visa products or services or impair the reputation or goodwill of Visa or the goodwill associated with the Marks
- Not refer to Visa in stating eligibility for its products, services, or membership

In addition, a Member or Visa Checkout Merchant that uses the Visa Checkout Mark must not use it as a substitute for the Visa-Owned Mark to indicate payment acceptance.

An Acquirer must ensure that a Merchant using any Visa-Owned Mark complies with the *Visa Product Brand Standards.*

ID# 0026991	Edition: Apr 2020 | Last Updated: Oct 2016

3.2.1.2   V PAY Brand Mark Use

The V PAY Brand Mark is a Visa-Owned Mark. Implementation of the V PAY Product and use of the V PAY Brand Mark outside the Europe Region is subject to approval and trademark availability. The V PAY Brand Mark must appear exactly as specified in the *Visa Product Brand Standards.*

ID# 0003585	Edition: Apr 2020 | Last Updated: Oct 2016

3.2.1.3   Use of the Visa Brand Name and the Visa Brand Mark on Merchant Websites and Applications

A Merchant website and/or application must display the Visa Brand Mark in full color, as specified in the *Visa Product Brand Standards.*

The Visa Brand Name must be used to indicate acceptance only when a visual representation of the Visa Brand Mark is not possible on the website or application.

A Merchant that displays the Visa Secure badge on its website or application must comply with the *Visa Product Brand Standards*.

A Merchant that retains Stored Credentials must display on the payment screen and all screens that show Payment Credential information both:

- The last 4 digits of the Payment Credential
- The Visa Brand Mark or the name "Visa" in text immediately next to a Visa payment option

ID# 0008671	Edition: Apr 2020 | Last Updated: Apr 2020

3.2.2   Use of Marks in Promotions, Advertisements, and Solicitations

3.2.2.1   Card and Product Positioning

An Issuer must refer to its Visa Card as a "Visa Card" in all communications regarding its program, including solicitations, advertising, promotions, and other Collateral Material.

ID# 0003211	Edition: Apr 2020 | Last Updated: Oct 2014

3.2.2.2   Limited Acceptance Merchant Signage

A Limited Acceptance Merchant may use the signage associated with the Limited Acceptance category it has selected, on promotional, printed, or broadcast materials only to indicate the types of Cards it accepts for payment.

ID# 0030376	Edition: Apr 2020 | Last Updated: Apr 2018

3.2.2.3   Non-Member Marks on Collateral Material – Canada Region

In the Canada Region: Except as permitted by Visa, a name, Trade Name, or Mark of a non-Member must not be used on Collateral Material bearing the Visa Program Marks that is used for soliciting applications or communicating with Cardholders.

This does not apply to the Marks of the Interac Association.

ID# 0006236	Edition: Apr 2020 | Last Updated: Oct 2014

3.2.2.4   Advertising Materials – Canada Region

In the Canada Region: Point-of-Transaction advertising and promotional materials (except credit card application forms) must not indicate that the Merchant has been signed by, or represents the interests of, a particular Member.

ID# 0006233	Edition: Apr 2020 | Last Updated: Oct 2014

3.2.3   Use of Marks on Cards

3.2.3.1   Hierarchy of Visa-Owned Marks on Cards

If more than one Visa-Owned Mark is present on a Card, an Issuer must designate a Primary Mark, complying with the following hierarchy of Marks:

- Visa Brand Mark
- Visa Brand Mark with the Electron Identifier
- Plus Symbol

All other Visa-Owned Marks must both:

- Appear together
- Not be separated by any non-Visa-Owned Marks

ID# 0008218	Edition: Apr 2020	Last Updated: Oct 2016

3.2.3.2   Prohibition of Non-Visa Payment Functionality on Visa Cards

A Member must not use a Functional Type or any other Mark on a Visa Card to facilitate payment for goods or services. This includes any mixture of alphanumeric characters that denotes participation in a program or benefit (for example: a loyalty or rewards program, a membership identification number).

In the Europe Region: A Member must provide Visa with details of the exact functionality of the Functional Type or Functional Graphic.

ID# 0029511	Edition: Apr 2020	Last Updated: Apr 2017

3.2.3.3   Use of Other Marks – US Region and US Territories

In the US Region or a US Territory: A Member must comply with the _Visa Product Brand Standards_ and _Table 3-1, Specific Marks Requirements – US Region and US Territories._

Table 3-1: Specific Marks Requirements – US Region and US Territories

Card Type	Marks	Allowed?
Visa Card that primarily accesses a line of credit	Interlink Program Marks	No
US Covered Visa Debit Card	Marks of a non-Visa general purpose payment card network	Yes
US Covered Visa Debit Card	Non-Visa-owned brand Marks	Yes, to indicate acceptance at Merchant Outlets solely within the country of Card issuance. The Marks must be equally prominent with or less prominent than the Visa Brand Mark.
US Covered Visa Debit Card	Marks that are specifically related to bank card programs and/or services related to those programs	Yes
US Covered Visa Debit Card	Marks of the American Express Company, Discover Financial Services, MasterCard Worldwide	Yes

Table 3-1: Specific Marks Requirements – US Region and US Territories (continued)

Card Type	Marks	Allowed?
	(including Maestro) or the subsidiaries or affiliates of these entities deemed competitive by Visa	
US Covered Visa Debit Card bearing the Plus Symbol	Marks of entities deemed competitive by Visa	Yes
Card not defined as US Covered Visa Debit Card	Marks that are specifically related to bank card programs and/or services related to those programs, unless the Visa Rules expressly allow them	No

ID# 0026531   Edition: Apr 2020 | Last Updated: Oct 2016

3.3   Other Card Requirements

3.3.1   Magnetic-Stripe Encoding

3.3.1.1   Magnetic-Stripe Encoding Requirements

The Magnetic Stripe on a Card must be encoded on both track 1 and 2.

In the LAC Region: This does not apply for Magnetic-Stripe personalization of embossed instant-issue Cards.

In the US Region: This does not apply for the Magnetic Stripe used to facilitate closed-loop campus applications on dual Magnetic-Stripe Campus Cards.

ID# 0003602   Edition: Apr 2020 | Last Updated: Apr 2020

3.3.1.3   Magnetic-Stripe Encoding – Europe Region (Germany)

In the Europe Region (Germany): An Issuer must encode the Magnetic-Stripe on all Cards using 2750 oersted high coercivity encoding technology, as specified in the industry standards adopted by Visa-approved manufacturers and Magnetic-Stripe encoding equipment providers.

ID# 0030043   Edition: Apr 2020 | Last Updated: Oct 2017

3.4   Point-of-Transaction Display of Marks

3.4.1   Display of Marks at the Point of Sale

3.4.1.1   Improper Display of Affinity/Co-Brand Partner Trade Name or Mark

Upon Notification from Visa, a Merchant must correct any display of an Affinity/Co-Brand partner's Trade Name or Mark at a Merchant Outlet if the display adversely affects the Visa brand.

ID# 0027375	**Edition: Apr 2020 | Last Updated: Oct 2015**

3.4.1.2   Display of Marks at Point of Payment Choice for Electronic Commerce and Payment Applications

A Merchant website and/or application must display at the point of payment choice the Visa POS graphic in full color, as specified in the _Visa Product Brand Standards._

ID# 0002337	**Edition: Apr 2020 | Last Updated: Apr 2017**

3.4.1.3   Display of Marks at the Point-of-Sale

The Visa-Owned Marks must not appear less prominently than any other payment Marks.[1]

A Merchant must display the Visa POS graphic prominently, as follows:

- At the Merchant entrance or storefront
- On the payment Acceptance Device, as specified in the _Visa Product Brand Standards_

[1] In the US Region or a US Territory: This does not apply.

ID# 0030002	**Edition: Apr 2020 | Last Updated: Oct 2017**

4   Issuance

4.1   General Issuance

4.1.1   General Issuer Requirements

4.1.1.1   Card and Token Positioning

An Issuer must not:

- Position any Visa Card as something other than a Visa Card. A Card that facilitates additional functionality or provides access to applications or services must still be positioned as a Visa Card[1]

- Position a Visa Business Card, Visa Corporate Card, or Visa Purchasing Card as something other than a Card for the payment of business expenditures

- Position its Trade Name or Mark as adding superior acceptance of the Card at the Point-of-Transaction[2]

An Issuer must ensure that a Token both:

- Maintains the same product characteristics of the Card represented by that Token

- Is presented to the Cardholder as a Visa product or service

If an Issuer provisions a non-Visa payment credential[3] for a co-resident network on a Card, it must also both:

- Provision a Visa Token before or at the same time as the non-Visa payment credential[3]

- Ensure that the applicable Token Requestor has received Visa Token Service approval of its digital wallet or other payment solution

[1] For example, a Card with added functionality such as Cardholder identification, participation in a loyalty program, or membership in an organization or, in the US Region, a Campus Card that facilitates closed-loop proprietary college or university transactions, must still be positioned as a Visa Card.

[2] This does not apply to discounts, promotional offers, or in-kind incentives offered by the Merchant.

[3] A token or other payment credential generated for a non-Visa general purpose payment card network that is co-resident on a Card and uses a BIN to identify the payment card within that co-resident payment card network.

ID# 0006153   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.1.2   Delivery of Visa Premium Product Value to Cardholders – AP, Canada, CEMEA, Europe, and LAC Regions

In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: An Issuer must structure its Visa premium products to deliver product value based on features, performance standards, and spending limits, such that:

- A Visa Infinite Card and a Visa Signature Card delivers higher value than a Visa Platinum Card.
- A Visa Platinum Card delivers equal or higher value than a Visa Gold/Premier Card.
- A Visa Gold/Premier Card delivers higher value than a Visa Classic Card.
- A Visa Business Gold Card delivers higher value than a Visa Business Card.
- In the Canada Region: A Visa Platinum Prepaid Card delivers higher value than a Prepaid Card
- **Effective 18 July 2020** In the Europe Region: A Visa Infinite Business Card delivers higher value than a Visa Platinum Business Card.
- **Effective 18 July 2020** In the Europe Region: A Visa Platinum Business Card delivers higher value than a Visa Business Card or a Visa Platinum Card.

ID# 0008225	**Edition: Apr 2020 | Last Updated: Apr 2020**

4.1.1.3   Non-Standard Card Prohibitions

An Issuer of a non-standard Card must not:

- Permit exclusive or preferential acceptance by a Merchant[1]
- Link the non-standard Card to a Virtual Account

In the Europe Region: A non-standard Card issued within the European Economic Area (EEA) must identify the correct Product Category on the Chip.

[1] This does not apply to discounts, promotional offers, or in-kind incentives offered by the Merchant.

ID# 0003242	**Edition: Apr 2020 | Last Updated: Oct 2016**

4.1.1.4   Issuer Requirements for a Credit Authorization on Returned Purchases

An Issuer must comply with the following Credit Authorization Requirements on returned purchases:[1]

Table 4-1: Credit Authorization Requirements

Region	Requirements
Effective through 17 April 2020 AP Region, Canada Region, CEMEA Region, LAC Region, US Region **Effective 18 April 2020** All Regions	Be prepared to receive and respond to an Authorization Request for a Credit Transaction
Effective through 17 April 2020 AP Region, Canada Region, CEMEA Region, LAC Region, US Region **Effective 18 April 2020** All Regions	Process the Credit Transaction so that Cardholder-facing applications are updated with the pending credit information in the same time frame as a purchase Transaction

[1] This is optional for Non-Reloadable Prepaid Cards.

ID# 0029557   **Edition: Apr 2020 | Last Updated: Apr 2019**

4.1.1.5   Issuance of Domestic Use-Only Cards – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, US Region: An Issuer must not issue a consumer Credit Card or a consumer Debit Card that is restricted to use only in the country of issuance. With prior Visa approval, an Issuer may issue a Prepaid Card that is restricted to use only in the country of issuance.

In the LAC Region: An Issuer must not do any of the following:

- Issue a consumer Credit Card or consumer Debit Card that is restricted to use only in the country of issuance. This does not apply to the following:
  - A Card issued under a Visa Program in existence before 13 October 2017 by an Issuer in the Dominican Republic, Haiti, Paraguay, or Uruguay
  - A Card issued in Argentina, Barbados, Chile, Colombia, Jamaica, or Trinidad
- In Brazil: Issue a Visa Consumer Card, Visa Commercial Card, or Visa Electron Card that is restricted to use only in the country of issuance
- In Mexico: Issue a consumer Credit Card, consumer Debit Card, or Visa Electron Card that is restricted to use only in the country of issuance

In the LAC Region: With prior Visa approval, an Issuer may issue a Prepaid Card that is restricted to use only in the country of issuance.

ID# 0029327   **Edition: Apr 2020 | Last Updated: Apr 2020**

4.1.1.6   Mailing of Individual Personalized Visa Products

An Issuer must do all of the following:

- Proof and prepare Visa Products for mailing under dual control in a high-security area separate from other operations
- Prevent unauthorized entry into the area
- Ensure that Cardholder addresses, including postal codes, are complete and correct
- Maintain stuffed, sealed, and stamped envelopes in a vault under dual control until mailing
- Record the exact date, time, and place of mailing for each Visa Product
- Report any Visa Products lost in the mail to Visa, the postal authorities, and the appropriate carrier

ID# 0025519   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.1.8   General Member Card Plan – Canada Region

In the Canada Region: Each Visa Canada General Member must operate its own Card plan that conforms to all of the following minimum standards:

- Each Member must issue Cards in its own name and own the receivables arising from the use of such Cards. Securitization does not impact ownership for the purpose of the Visa Rules.
- Cards issued by each Member will entitle Cardholders to make purchases of goods and services and to obtain Cash Disbursements.
- Subject to appropriate Authorization, each Member will honor Cards issued by other Members for Cash Disbursements.
- Subject to appropriate Authorization, each General Member will cause its Merchants to honor Cards issued by other such Members for the purchase of goods and services.

ID# 0004092   Edition: Apr 2020 | Last Updated: Oct 2014

4.1.1.9   Product Category Identification Requirements – Europe Region

In the Europe Region: An Issuer must identify a newly issued or reissued Card that is issued within the European Economic Area (EEA) by the correct Product Category, as specified in the *Visa Product Brand Standards* and *Table 4-2, Product Category Identification – Europe Region*.

An Issuer may identify a Card issued outside the EEA by the correct Product Category, as specified in the *Visa Product Brand Standards* and *Table 4-2, Product Category Identification – Europe Region*.

Table 4-2: Product Category Identification – Europe Region

Product Category	Debit	Credit (including Deferred Debit)	Prepaid
Interchange Fee Category	Consumer Immediate Debit	Consumer Credit	Consumer Immediate Debit
BIN Category	Debit	Credit or Deferred Debit	Prepaid

In France: Visa Affaires Cards that use the "EN" corporate product sub-type must be identified with:

- The credit Product Category
- The EMVCo-allocated "Application Product Identifier" tag value that identifies the product as credit

ID# 0029610	Edition: Apr 2020	Last Updated: Oct 2017

4.1.1.10   Issuer Requirements for Gambling Transactions in Norway – Europe Region

In the Europe Region (Norway): An Issuer must ensure that Cards issued in Norway are not used for gambling Transactions outside of Norway.

ID# 0030011	Edition: Apr 2020	Last Updated: Apr 2017

4.1.1.11   Card Accessing Cardholder Funds on Deposit – US Region

In the US Region: An Issuer must not issue or reissue a Card that accesses Cardholder funds on deposit at an organization other than the Issuer's, unless it both:

- Receives prior written consent from the organization where the funds are deposited
- Completes automated clearing house notification requirements

This prohibition does not apply to monthly periodic payments by the Cardholder to the Issuer.

ID# 0004573	Edition: Apr 2020	Last Updated: Apr 2020

4.1.1.12   Card Verification Value 2 (CVV2) Issuer Requirements – US Region

In the US Region: An Issuer must provide Visa with valid CVV2 encryption keys and test Account Numbers with CVV2 values and expiration dates.

ID# 0000672	Edition: Apr 2020	Last Updated: Oct 2014

4.1.1.13   Positioning, Acceptance, and Accounts – US Region

In the US Region: An Issuer must not:

- Designate or design any of its Cards, whether through the use of a Trade Name, Mark, numbering scheme, code on the Magnetic Stripe or Chip, QR code, or any other device or means, in order to either:

    – Permit exclusive or preferential acceptance of any of its Cards by any Merchant. This does not apply to discounts, promotional offers, or in-kind incentives offered by the Merchant.

    – Allow any Transaction involving use of these Cards to be treated as anything other than a Visa Transaction, except as specified in *Section 7.1.4, Non-Visa Debit Transaction Disclosure Requirements – US Region*[1]

- Allow a Card that is used primarily to access a line of credit to participate in any PIN-based debit program, unless the participation is for ATM access only

[1] This does not apply to Campus Cards that facilitate closed-loop proprietary college or university system transactions and permit the use of campus identification/access applications. A Campus Card must still be positioned as a Visa Card, but with additional functionality.

ID# 0003210 | **Edition: Apr 2020 | Last Updated: Apr 2020**

4.1.1.14   Marketing Materials for Visa Products

An Issuer must receive written approval from Visa before distribution of marketing materials, as follows:

Table 4-3: Marketing Materials Approvals for Visa Products

Applicable Products	Issuer Region	Requirements
Visa Signature	AP Region, CEMEA Region, US Region	- In the AP Region: Includes all Cardholder communication materials - In the CEMEA Region: Includes all marketing materials - In the US Region: Includes Visa Signature marketing materials, customer communications, terms and conditions, and/or disclosures
Visa Signature Preferred	US Region	Includes Visa Signature Preferred marketing materials, customer communications, terms and conditions, and/or disclosures

Table 4-3: Marketing Materials Approvals for Visa Products (continued)

Applicable Products	Issuer Region	Requirements
Visa Infinite	All Regions	• Includes Merchant partnership and emergency services material • Additionally in the AP Region and Canada Region, includes all Cardholder communication materials
Visa Infinite Privilege	Canada Region	Includes marketing materials for its Cardholders with terms and conditions and/or disclosures
Visa Platinum Business	CEMEA Region, Europe Region[1]	All Cardholder communication material
Visa Signature Business	AP Region and CEMEA Region	• In the AP Region: Includes Cardholder communication material relating to Merchant partnership or emergency services • In the CEMEA Region: Includes all marketing materials
Visa Infinite Business	AP Region, Canada Region, Europe Region[1]	• In the AP Region, Europe Region[1]: Includes all Cardholder communication materials • In the Canada Region: Includes Cardholder communication material relating to Merchant partnership or emergency services
Visa Infinite Corporate	LAC Region	Includes Merchant partnership and emergency services material for the Cardholders

[1] **Effective 18 July 2020**

ID# 0029988	**Edition: Apr 2020	Last Updated: Apr 2020**

4.1.1.15   Visa Card Customer Service Requirements

An Issuer must provide to its Cardholders customer service that is available 24 hours a day, 7 days a week to obtain emergency and account-related information services.[1]

[1] Optional for Visa Electron, Visa Classic, and Non-Reloadable Prepaid Cards

ID# 0029989	**Edition: Apr 2020	Last Updated: Apr 2020**

4.1.1.16   Presence of Payment Account Reference

A Visa payment account must have an associated Payment Account Reference.

| ID# 0030037 | Edition: Apr 2020 \| Last Updated: Oct 2018 |

4.1.1.17   Card Personalization – Europe Region (Germany)

In the Europe Region (Germany): An Issuer must ensure that all Cards are personalized to support Cash-Back.

| ID# 0030121 | Edition: Apr 2020 \| Last Updated: Apr 2018 |

4.1.2   Visa Credit Card Issuance

4.1.2.1   Second Line of Credit for On-Us Transactions – LAC Region

In the LAC Region: An Issuer's offer of a second line of credit must comply with all of the following:

- Be offered only in association with an Affinity/Co-Brand partner
- Be restricted to purchase Transactions completed as Visa Transactions at the Affinity/Co-Brand partner's Merchant Outlet
- Be restricted to On-Us Transactions
- Not exceed the amount of primary line of credit

| ID# 0007302 | Edition: Apr 2020 \| Last Updated: Oct 2015 |

4.1.2.2   Visa Consumer Product Core Card Benefits – LAC Region

In the LAC Region: A Visa Consumer Card Issuer must, at a minimum, provide its Cardholders with all of the following core product benefits, unless prohibited by applicable laws or regulations:

Table 4-4: Visa Consumer Product Core Card Benefits – LAC Region

Core Benefit	Visa Classic[1,2]	Visa Gold	Visa Platinum	Visa Signature	Visa Infinite
Travel Information Services	Worldwide	Worldwide	Worldwide	Worldwide	Worldwide
Price Protection	Minimum USD	Minimum USD	Minimum USD	Minimum USD	Minimum USD

Table 4-4: Visa Consumer Product Core Card Benefits – LAC Region (continued)

Core Benefit	Visa Classic[1,2]	Visa Gold	Visa Platinum	Visa Signature	Visa Infinite
	25 price difference per item up to USD 200 per account, per year	25 price difference per item up to USD 400 per account, per year	25 price difference per item up to USD 2,000 per account, per year	25 price difference per item up to USD 2,000 per account, per year	25 price difference per item up to USD 4,000 per account, per year
Purchase Protection	N/A	Up to USD 1,000 per account, per year	USD 5,000 per item up to USD 10,000 per account, per year	USD 5,000 per item up to USD 10,000 per account, per year	USD 10,000 per item up to USD 20,000 per account, per year
Extended Warranty	N/A	USD 1,000 per item up to USD 5,000 per account, per year	USD 5,000 per item up to USD 10,000 per account, per year	USD 5,000 per item up to USD 10,000 per account, per year	USD 5,000 per item up to USD 25,000 per account, per year
Auto Rental Insurance	N/A	Worldwide, including country of residence[3]	Worldwide, including country of residence	Worldwide, including country of residence	Worldwide, including country of residence
International Emergency Medical Services	N/A	N/A	Up to USD 150,000	Up to USD 200,000	Up to USD 200,000
Baggage Delay	N/A	N/A	N/A	USD 500 per beneficiary, per event	USD 600 per beneficiary, per event
Baggage Loss	N/A	N/A	N/A	Up to USD 1,000 per beneficiary, per event	Up to USD 3,000 per beneficiary, per event
Missed Connection	N/A	N/A	N/A	N/A	Up to USD 300

Table 4-4: Visa Consumer Product Core Card Benefits – LAC Region (continued)

Core Benefit	Visa Classic[1,2]	Visa Gold	Visa Platinum	Visa Signature	Visa Infinite
Trip Delay	N/A	N/A	N/A	N/A	Up to USD 300 more than 4 hours of delay
Trip Cancellation	N/A	N/A	N/A	N/A	Up to USD 3,000
Personal Concierge Service	N/A	N/A	Provided through Visa	Provided through Visa	Provided through Visa
Priority Pass Membership	N/A	N/A	N/A	N/A	Complementary membership for Core Priority Pass programs

[1] In Mexico: This does not apply to Visa Classic Cards issued as Debit Cards.

[2] In Brazil: This does not apply to Visa Classic Cards.

[3] This does not apply to Visa Gold Cards issued as Debit Cards.

ID# 0029542   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.3   Visa Charge Card Issuance

4.1.3.1   Visa Charge Card Classification

An Issuer must identify a Visa Charge Card and distinguish it from a Visa Consumer Credit Card by using one of the following classification levels:

- BIN
- Account Range Definition (ARDEF)
- Registered Program Identification Number (RPIN)
- Account Level Processing

ID# 0026357   Edition: Apr 2020 | Last Updated: Apr 2019

4.1.3.2   Visa Charge Card Authorization Requirements – US Region

In the US Region: A Visa Charge Card issued as a Visa Signature Card or Visa Signature Preferred Card must be issued with no pre-set spending limit.

ID# 0026981	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.3.3   Visa Charge Card Issuer Registration – AP and US Regions

In the AP Region, US Region: A Visa Charge Card Issuer must register its Visa Charge Card program and obtain prior approval from Visa.

ID# 0026356	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.4   Debit Card Issuance

4.1.4.1   Debit Card Issuer Cash-Back Requirements – US Region

In the US Region: A Debit Card Issuer and Visa Business Check Card Issuer must support the Visa Cash-Back Service.

This requirement does not apply to certain Prepaid Cards, as specified in *Section 1.4.4.1, PIN Issuance*.

ID# 0026502	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.4.2   Debit Card Partial Preauthorization – US Region

In the US Region: A Debit Card Issuer or Visa Business Check Card Issuer and its VisaNet Processor must support partial preauthorization Responses for PIN-Authenticated Visa Debit Transactions.

ID# 0026503	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.4.3   Consumer Deferred Debit Card Equivalent – US Region

In the US Region: An Issuer must position a consumer deferred Debit Card only as a Card that accesses a consumer's deposit, investment, or other asset account, including a fiduciary account, where the amount of any individual Transaction is not accessed, held, debited, or settled from the consumer asset account sooner than 14 days from the date of the Transaction.

A consumer deferred Debit Card is treated as a Credit Card only for Limited Acceptance purposes.

ID# 0004153   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.4.4   Visa Debit Category Transaction Identification – Canada Region

In the Canada Region: A Visa Debit Category Card Issuer must both:

- Identify all Visa Debit Category Transactions as Visa Transactions in all communications displaying Transaction information, including account activity statements
- Clearly disclose to the Cardholder any distinction between a Visa Debit Category Transaction and other payment services

ID# 0008073   Edition: Apr 2020 | Last Updated: Oct 2014

4.1.4.5   Visa Debit Category Issuer Chip Requirements – Canada Region

In the Canada Region: A Visa Debit Category Issuer must ensure that the Visa Application Identifier (AID) is present on the Card and the Application Selection Flag (ASF) settings comply with the *Visa Canada Debit Card – Technical Specifications*.

ID# 0008072   Edition: Apr 2020 | Last Updated: Oct 2014

4.1.6   Affinity/Co-Brand and Global Co-Brand Issuance

4.1.6.1   Co-Branding Partnership Approval Documentation Requirements

A Global Co-Branding Partner and Issuer must provide a dossier of proprietary and public information for approval to Visa, including both:

- *Co-Branding Partnership Regional Approval Form* for each proposed interregional and intraregional co-branding program
- Global Co-Branding Partners' Marks and design guidelines (including color proofs) or evidence that a trademark search has been conducted

ID# 0004052   Edition: Apr 2020 | Last Updated: Oct 2014

4.1.6.2   Global Co-Branding Partner Eligibility

A Global Co-Branding Partner must comply with all of the following:

- Be sponsored by an Issuer
- Not be an entity deemed to be a competitor of Visa

- In the Europe Region: Not be eligible for Visa membership. This does not apply to Prepaid Cards.

ID# 0004053	Edition: Apr 2020	Last Updated: Apr 2020

4.1.6.3   Global Co-Branding Issuer Qualification and Notification

An Issuer that partners with a Global Co-Brand Partner must both:

- Be a qualified Issuer in countries where Global Co-Brand Cards will be issued
- Notify Visa of its plans to expand interregional and intraregional Global Co-Brand Partners

ID# 0004055	Edition: Apr 2020	Last Updated: Oct 2015

4.1.6.4   Affinity/Co-Branded Card Program Requirements

An Affinity/Co-Brand Card Issuer must do all of the following:

- Submit a completed Affinity/Co-Brand Application and obtain written approval from Visa for each Affinity/Co-Brand program before issuing Affinity/Co-Brand Cards
- Only issue Affinity/Co-Brand Cards to residents of the Visa Region in which the Issuer is located
- In the Europe Region: All of the following:
    - Identify an Affinity/Co-Brand program using an eligible Account Range
    - Notify Visa in the Affinity/Co-Brand Application which Account Range corresponds to which Affinity/Co-Brand program
    - Require the Affinity/Co-Brand partner to submit written agreement to the Issuer acknowledging the rights of Visa to the Visa-Owned Marks

If requested by Visa, the Issuer must provide additional documentation, including all of the following:

- The agreement between the Issuer and the Affinity/Co-Brand partner
- Collateral Material
- Information regarding the reputation and financial standing of the Affinity/Co-Brand partner
- Other documentation

In the Canada Region: A General Member and Affinity/Co-Brand partner must complete all required documentation and agreements required by the applicable Mark owners.

ID# 0027363	Edition: Apr 2020	Last Updated: Oct 2019

4.1.6.5 Visa Requests for Affinity/Co-Brand Program Information

A Member must submit both of the following to Visa upon request to determine compliance with Affinity/Co-Brand program requirements:

- Any and all contracts with the Affinity/Co-Brand partner

- Any other documentation relative to the Affinity/Co-Brand program

ID# 0027373	Edition: Apr 2020 | Last Updated: Oct 2015

4.1.6.6 Affinity/Co-Brand Partner Eligibility Requirements

An Affinity/Co-Brand partner must not be an organization that is deemed to be a competitor of Visa.

To display the Marks of another Member or a non-Member that is engaged in banking activities and eligible for Visa membership as an Affinity/Co-Brand partner on its Cards,[1] an Issuer must do all of the following:

- Obtain prior approval from Visa

- Clearly identify itself as the Issuer on the Card and program materials

- Ensure that the Affinity/Co-Brand program is established solely to distribute or sell Cards. The Affinity/Co-Brand partner must act only as the distributor/reseller.

- Maintain complete control over the Affinity/Co-Brand Cards, including responsibility for customer service and assumption of financial liability. The Affinity/Co-Brand partner must not be engaged in an ongoing contractual relationship with the Cardholder in connection with the Issuer's Card.

- For Prepaid Cards, assume complete responsibility for oversight and control of its Affinity/Co-Brand partner, as specified in *Section X*.

In the Europe Region: If an Affinity/Co-Brand partner is a retailer, its Merchant Outlets must accept Cards.

[1] In the Europe Region: This is allowed only for Prepaid Cards.

ID# 0027364	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.6.7 Affinity/Co-Brand Program Ownership and Control

An Issuer that partners in offering an Affinity/Co-Brand program must comply with all of the following:[1]

- Underwrite, issue, and maintain the account associated with an Affinity/Co-Brand Card

- Always be portrayed as the owner of the Affinity/Co-Brand program

- Own and control an Affinity/Co-Brand program as defined by Visa on the basis of the Issuer's entire relationship with the Affinity/Co-Brand partner, including all of the following:

  – Whether the Issuer controls, or exercises controlling influence over, the management policies with respect to the Affinity/Co-Brand program

  – The extent to which the Issuer conducts credit evaluations, participates in Cardholder billing, or provides customer services in connection with the Affinity/Co-Brand program

  – Whether all or part of the receivables are financed by the Affinity/Co-Brand partner

[1] In the AP Region (Australia): This does not apply to mortgage originator programs, pastoral companies, and superannuation funds.

ID# 0027365	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.6.8   Affinity/Co-Branded Card Transaction Processing

A Transaction completed with an Affinity/Co-Branded Card (including an On-Us Transaction) must be processed and treated as a Visa Transaction.

In the AP Region (Japan): This does not apply to Cards issued with multiple Magnetic Stripes

In the Europe Region: This does not apply to Cards issued with 2 or more payment scheme brands

In the US Region: This does not apply to Campus Cards that facilitate closed-loop proprietary college or university system transactions and permit the use of campus identification/access applications. A Campus Card must still be positioned as a Visa Card.

In the US Region: This does not apply, as specified in *Section 7.1.1.4, Non-Visa Debit Transaction Disclosure Requirements – US Region*.

ID# 0027370	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.6.9   Affinity/Co-Branded Card Account Access

An Affinity/Co-Branded Card must not be used to debit any credit, charge, payment, or deposit account other than the account maintained by the Issuer in connection with that Affinity/Co-Branded Card.

In the AP Region (Japan): This does not apply to Cards issued with multiple Magnetic Stripes.

In the LAC Region: This does not apply as specified in *Section 4.1.2.1, Second Line of Credit for On-Us Transactions – LAC Region*.

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

ID# 0027371	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.6.10   Affinity/Co-Branded Card Rules for Proprietary Cards Bearing the Plus Symbol

Affinity/Co-Branded Card rules do not apply to Proprietary Cards that display non-Member identification and bear the Plus Symbol, but no other Visa Mark.

ID# 0027372	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.6.11   Determination of Affinity/Co-Brand Program Violations

If Visa determines that any provisions of the Affinity/Co-Brand program requirements have been violated, Visa reserves the right to both:

- Require modification of the program, including both:
  - Assignment of the program to a third party
  - Suspension of the program
- Impose non-compliance assessments or terminate the program with 90 calendar days' written notice

ID# 0027374	Edition: Apr 2020 | Last Updated: Oct 2015

4.1.6.12   Co-Brand Partner Contract Requirements – Europe Region

In the Europe Region: A Member must include a provision in its contracts with a Co-Brand Partner that specifies that the Co-Brand Partner must not misrepresent itself as being a Member.

ID# 0029801	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.7   Card Production Standards

4.1.7.2   Cardholder Name on Chip and Magnetic Stripe – Europe Region

In the Europe Region: If the Cardholder name is encoded on the Chip and on the Magnetic Stripe on a Card, the names encoded must be the same as the name displayed on the Card as far as is allowed by the character sets supported by the Chip and the Magnetic Stripe.

ID# 0029641	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.7.4   Card Activation Stickers

With the exception of a Card activation sticker, an Issuer must not affix any adhesive material to the front or back of a Card unless it is integral to the manufacturing of the Card.

The Issuer must ensure that a Card activation sticker affixed to the front or back of its Card does not interfere with any security features of the Card.

The Card activation sticker or other material enclosed with the Card mailer must provide a method for the Cardholder to activate the Card upon receipt.

ID# 0008695	Edition: Apr 2020 | Last Updated: Apr 2018

4.1.7.5   Visa Mini Card Issuer Requirements

A Visa Mini Card Issuer must comply with all of the following:

- Issue the Visa Mini Card with the same expiration date as the standard-sized companion Card
- Issue the Visa Mini Card as the same Visa product type and with the same benefits as the standard-sized companion Card
- At the time of issuance, inform the Cardholder of potential usage restrictions
- In the US Region: Issue the Visa Mini Card in conjunction with a corresponding standard-sized Visa Card
- In the US Region: Not establish a daily Transaction amount limit for Visa Contactless Mini Card use

ID# 0027520	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.8   Virtual Accounts

4.1.8.1   Virtual Account Requirements

An Issuer that offers a Visa Virtual Account must comply with the electronic payment authentication requirements established by Visa.

ID# 0001643	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.8.2   Virtual Account Issuer Requirements

A Virtual Account Issuer must comply with all of the following:

- Obtain prior approval from Visa

- Use the BIN designated for the specific product or program for which a Virtual Account is issued

- Verify account information, including name of the Virtual Account owner, Payment Credential, account expiration date, and Card Verification Value 2 (CVV2) and communicate it securely to the Virtual Account owner

- If a Reference Card is provided, comply with Reference Card design requirements

- In the Europe Region: Report Virtual Account products on the Quarterly Operating Certificate

ID# 0001645	Edition: Apr 2020	Last Updated: Apr 2020

4.1.9   Issuer Disclosures

4.1.9.1   Issuer Disclosure of Authorization Request Amounts

If an Issuer includes information from an Authorization Request in an online Cardholder statement, Cardholder alert, or other communication to the Cardholder, it must both:

- Notify its Cardholder that an Estimated Authorization Request, Initial Authorization Request, or Incremental Authorization Request amount may differ from the final Transaction amount

- For an Automated Fuel Dispenser Transaction, not notify its Cardholder of the amount of the Authorization Request in the online Cardholder statement, Cardholder alert, or other communication. It may notify the Cardholder of the final Transaction amount from the Acquirer Confirmation Advice or the Completion Message.

ID# 0029466	Edition: Apr 2020	Last Updated: Oct 2017

4.1.9.2   Emergency Services Telephone Numbers

An Issuer must notify its Cardholders at least once each year of the availability of emergency services and provide a toll-free or international collect-call telephone number through which Cardholders may obtain these services.

ID# 0025791	Edition: Apr 2020	Last Updated: Apr 2019

4.1.9.3   Disclosure of Responsibility for Charges – AP Region

In the AP Region: A Member must not represent to its Cardholder or its Merchant that Visa imposes any charge on the Cardholder or the Merchant. A Member is responsible for making whatever disclosures applicable laws or regulations require with respect to its charges to its Cardholders or its Merchants.

ID# 0004089	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.9.4   Issuer Contact Disclosure – Canada Region

In the Canada Region: An Issuer must disclose in its consumer Cardholder agreements that a Cardholder may contact the Issuer to discuss disputes the Cardholder may have with respect to a Transaction on their statement.

ID# 0004106	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.9.5   Issuer Disclosure of Fees and Charges – CEMEA Region

In the CEMEA Region: An Issuer of Visa Cards, Proprietary Cards bearing the Plus Symbol, and Cards bearing the Visa Brand Mark with the Electron Identifier must notify its Cardholder in writing of the following:

- That the exchange rate between the Transaction Currency and the Billing Currency used for processing International Transactions is either:
  - A wholesale market rate
  - The rate mandated by a government or governing body
- Additional fees and charges (if any) assessed by the Issuer through the application of an Optional Issuer Fee to the Currency Conversion Rate or any other fees for currency conversion
- Specific fees and charges to be assessed to the Cardholder, where appropriate, including:
  - Annual fee
  - Interest rate(s), if applicable
  - ATM Cash Disbursement fee
  - Manual Cash Disbursement fee
  - PIN replacement charge
  - Fee for additional statement copies
  - Late payment fee
- Date on which the Cardholder will incur a late payment fee if the Issuer does not receive payment for outstanding Transaction amounts appearing on the Cardholder billing statement

An Issuer may choose the method by which it notifies the Cardholder in writing. This may include one or more of the following:

- Cardholder agreement
- Cardholder terms and conditions
- Any other agreement between the Cardholder and Issuer
- Monthly billing statement

ID# 0008822	Edition: Apr 2020	Last Updated: Apr 2016

4.1.9.6   Cardholder Agreement Requirements – Europe Region

In the Europe Region: Taking into account all the products and services provided by Visa, all information required under applicable data protection legislation must be provided in the Cardholder agreement including, but not limited to, the following:

- The identity of the Issuer
- The purposes for which the processing of any Personal Data is intended, including building a profile of the Cardholder's interests
- The recipients of the Personal Data, such as:
  - The Member's subsidiaries and/or group of companies, agents, and employees
  - Visa, its employees, and its third party subcontractors and their employees
  - Third parties with whom the Cardholder transacts and has agreed to share Personal Data
  - Third parties in an approved partnership with Visa, only where such data is presented in either an anonymized, pseudonymized, or aggregated form and will never be able to be used by those third parties to identify a particular Cardholder
  - Such other entities to which it may be reasonably necessary to disclose and transfer Personal Data (for example: credit reference agencies, law enforcement agencies, anti-terrorism or organized crime agencies, fraud monitoring agencies, central banks)
  - Any other entities, to be clearly specified as otherwise required or permitted by applicable laws or regulations
- That the transfer and disclosure of personal data may take place worldwide and that the transfer of Personal Data outside the European Economic Area (EEA) is on the basis of either:
  - Appropriate or suitable safeguards as required by applicable laws or regulations
  - An adequacy decision by the European Commission

Where the basis of the transfer is for appropriate or suitable safeguards, the Member is responsible for ensuring that Cardholders can have access to such appropriate or suitable safeguards.

- Any other information necessary to guarantee fair and transparent processing of Personal Data under applicable laws or regulations, including without limitation:
  - That aggregated, anonymized data may be created based on Personal Data
  - That data may be used and/or shared where deemed applicable with third parties for:
    - Billing purposes
    - Product enablement and build
    - Testing or product improvement purposes
    - To reply to requests from public authorities
  - That Cardholders are not identifiable from this data
  - That data may be analyzed by Visa and its partners for offers or promotional activities that Cardholders have entered or agreed to be a part of
  - The categories of Personal Data processed, whenever considered necessary for the legitimate interest pursued by the Member
  - A contact point for data protection-related enquiries and/or subject access requests

In addition, where a Member is located and/or issues a Card to a Cardholder located within the EEA, the Cardholder agreement must include all of the following:

- The identity of the Issuer as data controller and corresponding contact details (including a representative in the EEA, where the data controller is based outside the EEA
- The identity of any additional data controller and corresponding contact details
- The identity and contact details for the appropriate data protection officer
- The legitimate interest of the data controller where any processing is based on such interest
- The data storage period or, where not specific, the criteria used to determine that period
- All data rights available to the Cardholder, taking into account the relevant Visa services, including the right to lodge a complaint with an authority and, where applicable, the right to erasure and/or correction of Personal Data and data portability

ID# 0029614	Edition: Apr 2020 | Last Updated: Apr 2018

4.1.9.7   Cardholder Choice of Payment Scheme – Europe Region

In the Europe Region: For a Card issued inside the European Economic Area, an Issuer must include a provision in its Cardholder agreement to explain that when a Card supports more than one payment scheme and is used at a Merchant Outlet that accepts those payment schemes, the

Cardholder retains, at the Point-of-Transaction, complete discretion over the payment scheme that is used to initiate a Transaction.

This requirement does not apply to Transactions at an Unattended Cardholder-Activated Terminal with no Cardholder input interface.

ID# 0029615	Edition: Apr 2020 | Last Updated: Oct 2017

4.1.9.8   Communication of Change of Card Details – Europe Region

In the Europe Region: An Issuer must communicate to its Cardholder in writing any change in the Cardholder's Card details. This communication must both:

- Advise the Cardholder of the impact of changing Card details and any need for action
- Prompt the Cardholder to contact any Merchants with which it has either:
  - A Recurring Transaction agreement
  - An agreement to store the Cardholder's Stored Credential

ID# 0029814	Edition: Apr 2020 | Last Updated: Apr 2018

4.1.9.9   Issuer Disclosure Requirements – Europe Region

In the Europe Region: An Issuer must notify its Cardholders in writing of the following:

- Specific fees and charges to be assessed to the Cardholder, including, but not limited to:
  - Annual fee
  - Interest rate(s), if applicable
  - ATM Cash Disbursement fee
  - Manual Cash Disbursement fee
  - PIN replacement charge
  - Fee for additional billing statement copies
- Date on which Transactions will be debited from the Cardholder's account

ID# 0029815	Edition: Apr 2020 | Last Updated: Apr 2017

4.1.9.10   Card Application Processing Fee – US Region

In the US Region: An Issuer or Agent that charges a fee to a Cardholder for processing a Card application must comply with all of the following:

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

- Disclose the application processing fee as being separate from any other fees associated with use of the Card

- Provide the disclosure in a way that allows the Cardholder to avoid the fee if they do not want to pursue the application

The Issuer or its Agent must not:

- Charge a fee for providing an application to a prospective Cardholder

- Use a "900" area code, "976" telephone exchange, or any similar telephone number to indirectly charge a fee for inquiries about obtaining a Card

ID# 0000412	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.9.11   Disclosure of Card Features and Services – US Region

In the US Region: An Issuer must disclose to its Cardholders, in a timely manner, upgraded features and services when a Cardholder converts from one Card program to another (for example: Visa Traditional to Visa Signature). The Issuer is responsible for any liability that arises from the timing of the disclosure.

ID# 0000425	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.9.12   Communication of Cardholder Assistance Telephone Number – US Region

In the US Region: An Issuer must communicate one of the following toll-free telephone numbers to each Cardholder at least once a year:

- Visa Customer Care Services telephone or fax number

- Issuer's or its agent's assistance center telephone or fax number

The toll-free telephone number must be printed on material furnished to the Cardholder.

ID# 0008723	Edition: Apr 2020 | Last Updated: Oct 2019

4.1.10   Confidentiality of Cardholder Information

4.1.10.1   Cardholder Information Privacy Requirements – Canada Region

In the Canada Region: An Issuer must certify to Visa that it has met the applicable requirements of privacy legislation for the collection, use, and disclosure of personal Cardholder information among Visa and its employees and agents, for the purpose of processing, authorizing, and

authenticating a Cardholder's Transactions and providing customer assistance services to a Cardholder.

ID# 0001986	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.10.2   Contest and Promotion Privacy Requirements – Canada Region

In the Canada Region: An Issuer will have met the applicable requirements of privacy legislation where the Issuer's Cardholders participate in contests and promotions administered by Visa on behalf of the Issuer.

ID# 0001987	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.11   PIN Requirements

4.1.11.1   PIN as Cardholder Verification Method – Issuer Requirements – AP Region (India)

In the AP Region (India): An Issuer must have PIN as the preferred Cardholder Verification Method (CVM) for all newly issued or re-issued Debit Cards and Reloadable Prepaid Cards.

An Issuer must respond with a Decline Response when an Authorization Request for a Domestic Transaction conducted in a Card-Present Environment on a Debit Card or Reloadable Prepaid Card does not include a PIN or the confirmation that PIN was correctly entered.

ID# 0027954	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.11.2   PIN Verification Service Request – Europe Region

In the Europe Region: An Issuer must submit a written request to Visa at least 90 calendar days before implementing the PIN Verification Service.

ID# 0029592	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.11.3   PIN Verification Service – Issuer Requirements – US Region

In the US Region: If an Issuer uses the PIN Verification Service, the Issuer must either:

- Encode the PIN Verification Value on the Magnetic Stripe, and for Cards containing a Chip, both the Magnetic Stripe and Chip. This applies only if the Issuer requires Stand-In Processing to verify PINs.

- Ensure that the PIN Verification Value resides on the PIN Verification Value file maintained by Visa

ID# 0007045	Edition: Apr 2020	Last Updated: Oct 2015

4.1.11.5   PIN Issuance for Visa Signature and Visa Signature Preferred Cards – US Region

In the US Region: An Issuer must comply with *Section 1.4.4.2, PIN Issuance Requirements,* within one year of issuing either of the following Card products to a new Cardholder:

- Visa Signature
- Visa Signature Preferred

An Issuer whose internal systems support customer PIN selection must offer the availability of PINs to all of its Cardholders.

An Issuer whose internal systems do not support customer PIN selection must issue PINs to all of its Cardholders and not simply notify its Cardholders that PIN is available upon request.

ID# 0008126	Edition: Apr 2020	Last Updated: Oct 2014

4.1.11.6   PIN as Cardholder Verification Method – Europe Region (Slovakia)

In the Europe Region (Slovakia): For a Visa Electron Transaction in a Card-Present Environment, the primary Cardholder Verification Method must be PIN.

ID# 0030059	Edition: Apr 2020	Last Updated: Oct 2017

4.1.12   Data Retention and Transmission

4.1.12.1   Cardholder Data Provision for Prize Awards – US Region

In the US Region: An Issuer must provide Cardholder data to Visa for the purposes of awarding prizes in conjunction with promotional activities conducted by Visa.

If prohibited by applicable laws or regulations from disclosing Cardholder data, the Issuer must both:

- Notify the Cardholder of the awarded prize and obtain necessary documentation
- Ensure that the prize is awarded directly to the Cardholder

| ID# 0008704 | Edition: Apr 2020 \| Last Updated: Oct 2014 |

4.1.12.2   Enriched Transaction Data – US Region

In the US Region: An Issuer that receives enriched data with any of the following Transactions must either print the data on the Cardholder statement or retain the data for a minimum of 200 calendar days from the Transaction Date:

- CPS/Hotel and Car Rental Card Present
- CPS/Hotel and Car Rental Card Not Present
- CPS/e-Commerce Preferred Hotel and Car Rental
- A Transaction that includes Airline itinerary data or ancillary data

| ID# 0003554 | Edition: Apr 2020 \| Last Updated: Oct 2016 |

4.1.12.3   Issuer Requirements for Reporting Linked Consumer Credit Accounts – US Region

In the US Region: An Issuer with more than USD 1 billion in annual Visa Consumer Credit Card Transaction volume must link its Visa Consumer Credit Cards if the Payment Credentials are different, as follows:

- A secondary Card(s) to its primary Card through the Cardholder Maintenance File (CMF)
- A virtual Card(s) to its primary or secondary physical Card(s) through the CMF

| ID# 0029502 | Edition: Apr 2020 \| Last Updated: Apr 2020 |

4.1.13   Provisional Credit/Zero Liability

4.1.13.1   Provisional Credit

An Issuer must provide provisional credit for the amount of a dispute or an unauthorized Transaction (as applicable) to a Cardholder's account, as follows:

Table 4-5: Provision of Provisional Credit

Issuer Region	Product Type	Provisional credit must be provided to a Cardholder's account:	Additional Requirements / Allowances
AP Region	Visa Infinite	Within 24 hours of	The Issuer must do all of the following:

Table 4-5: Provision of Provisional Credit (continued)

Issuer Region	Product Type	Provisional credit must be provided to a Cardholder's account:	Additional Requirements / Allowances
	Visa Infinite Business	notification of a Cardholder dispute	• Place the disputed Transaction amount in a suspense account until the dispute is resolved • If the Merchant refutes the Dispute, inform the Cardholder and attempt to resolve the dispute • Send letter of explanation to the Cardholder when the dispute is resolved
	Visa Signature	Within 24 hours of notification of a Cardholder dispute	The Issuer must place the disputed Transaction amount in a suspense account until the dispute is resolved.
	Visa Ultra High Net Worth	Within 24 hours of notification of a Cardholder dispute	The Issuer must not assess finance charges on the disputed amount.
	All other Cards	Within 5 business days of notification, unless the Issuer determines that additional investigation is warranted	N/A
Canada Region	Debit Category	Within 2 business days of notification of a dispute or unauthorized Transaction, unless any of the following apply: • The Issuer determines the need for special investigation • Transaction type or prior account history warrants a delay • The nature of the	The Issuer must dispute the Transaction amount if any of the following conditions apply: • The dispute relates to an Electronic Commerce or Mail/Phone Order Transaction. • The Merchant has not refunded the Cardholder within 30 days of the Cardholder's attempt to resolve the dispute. • The Cardholder is not expected to receive a refund from any other entity, fund, or

Table 4-5: Provision of Provisional Credit (continued)

Issuer Region	Product Type	Provisional credit must be provided to a Cardholder's account:	Additional Requirements / Allowances
		Transaction justifies a delay in crediting the Cardholder's account	source for the disputed Transaction.
	All other Cards	When both of the following are confirmed: • The dispute meets the Dispute criteria • The dispute is determined to be legitimate	If the Issuer does not dispute the Transaction amount as required, the credit to the Cardholder's account must be final. The Issuer may reverse a provisional credit only if it properly initiated a Dispute that is determined by Visa to be invalid, except where the Dispute is determined by Visa to be valid on its merits and properly documented, but declined by reason of the Issuer's failure to meet a Visa requirement.
CEMEA Region	Visa Ultra High Net Worth	Within 24 hours of notification of a Cardholder dispute	The Issuer must not assess finance charges on the disputed amount.
LAC Region	Credit Debit	Within 24 hours of notification of a Cardholder dispute, unless any of the following apply: • The Issuer determines the need for special investigation • Transaction type or prior account history warrants a delay • The nature of the Transaction justifies a delay in crediting the Cardholder's account	The Issuer may place the disputed Transaction amount in a suspense account until the dispute is resolved.
	Prepaid	Within 5 business days of	N/A

Table 4-5: Provision of Provisional Credit (continued)

Issuer Region	Product Type	Provisional credit must be provided to a Cardholder's account:	Additional Requirements / Allowances
		notification of an unauthorized transaction, unless the Issuer determines that additional investigation is warranted and allowed by applicable laws or regulations	
US Region	Visa Business Check Debit, except for ATM Cash Disbursements	Within 5 business days of notification of an unauthorized Transaction, unless the Issuer determines that additional investigation is warranted and allowed by applicable laws or regulations	N/A
	Visa Infinite **Effective 18 April 2020** Visa Infinite Business	Immediately	The Issuer must do all of the following: ● Ensure that the disputed amount is not calculated as part of the total balance or displayed on Cardholder statements or account summaries ● If the Merchant refutes the Dispute, inform the Cardholder and attempt to resolve dispute ● Send letter of explanation to the Cardholder when the dispute is resolved ● Notify the Cardholder before the Transaction is reposted to the account if the Dispute is reversed[1] ● Not assess any finance charges on the disputed amount for the period of the dispute
[1] For a Member that participates in Enhanced Dispute Resolution, applies if the Issuer is responsible for the Dispute			

Table 4-5: Provision of Provisional Credit (continued)

Issuer Region	Product Type	Provisional credit must be provided to a Cardholder's account:	Additional Requirements / Allowances
		amount	

ID# 0029461	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.13.2   Advertising for the Zero Liability Program – Canada Region

In the Canada Region: Any promotional, advertising, or marketing language used for the Zero Liability Program must contain messaging, in the body of the promotional, advertising, or marketing language and not as a footnoted disclaimer, to the effect that Cardholders are responsible for ensuring that they protect their PIN.

ID# 0000397	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.14   Emergency Cash Disbursement, Emergency Card Replacement, Global Customer Assistance Services (GCAS)

4.1.14.1   Issuer Requirements for Using the Visa Global Customer Assistance Services (GCAS) for Emergency Cash Disbursement and Emergency Card Replacement

An Issuer that uses the Visa Global Customer Assistance Services (GCAS) for Emergency Cash Disbursements or Emergency Card Replacements must comply with all of the following:

- At least 30 calendar days before BID or BIN activation, submit to GCAS all required contact information
- Advise its Cardholders of the availability of an Emergency Cash Disbursement or Emergency Card Replacement, as applicable
- Provide Cardholders with a telephone number that is available worldwide 24 hours a day, 7 days a week for Emergency Cash Disbursements and Emergency Card Replacements. The telephone number may be either the:
  - Visa Global Customer Assistance Services (GCAS) telephone numbers
  - Issuer's own worldwide emergency services telephone number
- Designate one or more Emergency Service Locations

- Notify GCAS within 30 calendar days of any changes to an Emergency Service Location

- Notify GCAS at least 2 weeks before any change in its Emergency Cash Disbursement or Emergency Card Replacement contact

- Approve or deny a request from GCAS or a Cardholder within 2 hours of notification

- Approve a Status Check Authorization unless there is an issue with the validation of the track 1 or track 2 data on the Magnetic Stripe or the Full-Chip Data on the Emergency Card Replacement

- For Emergency Card Replacements, both:

  – Provide accurate Cardholder information, including the correct spelling of the Cardholder's name as it should appear on the Emergency Card Replacement and Cardholder verification data

  – Assume responsibility for each Emergency Card Replacement issued by GCAS when the Card is embossed and encoded both:

    ▪ According to the Issuer's instructions

    ▪ With a Stand-In Processing Account

ID# 0002627	Edition: Apr 2020 | Last Updated: Apr 2019

4.1.14.2   Emergency Cash Disbursement and Emergency Card Replacement Provision Requirements

An Issuer or the Issuer's agent must provide an Emergency Cash Disbursement and Emergency Card Replacement as specified in *Table 4-6, Provision of Emergency Cash Disbursements to Cardholders,* and *Table 4-7, Provision of Emergency Card Replacements to Cardholders* except under the following circumstances:

- Delivery to the requested country is prohibited by applicable laws or regulations (for example: the country is embargoed).

- The Cardholder failed to provide accurate delivery information.

- Clearance through the country's international customs office is delayed.

- The destination is remote and not easily reachable.

- The Issuer or the Issuer's agent and the Cardholder have agreed to a specific delivery timeframe.

The Issuer or the Issuer's agent must not assess additional charges to the Cardholder if a service or timeframe is required for the Card type, as specified in *Section 4.1.14.5, Visa Global Customer Assistance Services Provision Requirements.*

Table 4-6: Provision of Emergency Cash Disbursements to Cardholders

Card Type	If Cardholder location is within the issuing Visa Region	If Cardholder location is outside the issuing Visa Region
Visa Classic, Visa Electron	Within 1 business day from the time that the Issuer approves the request	Within 1 business day from the time that the Issuer approves the request
Visa Gold/Premier, Visa Rewards, Visa Platinum, Visa Business, Visa Business Electron, Visa Corporate, Visa Purchasing	Within 24 hours from the time that the Issuer approves the request	Within 1 business day from the time that the Issuer approves the request
Visa Infinite (including Visa Infinite Business),[1,2,3] Visa Signature (including Visa Signature Business), Visa Infinite Privilege, Visa Ultra High Net Worth	Within 24 hours from the time that the Issuer approves the request	Within 24 hours from the time that the Issuer approves the request

[1] In the Canada Region: A Visa Infinite Privilege Issuer must offer an Emergency Cash Disbursement for a lost, stolen, or damaged Card reported by the Cardholder.

[2] In the US Region: A Visa Infinite Card Issuer must offer an Emergency Cash Disbursement for a lost, stolen, or damaged Card reported by the Cardholder.

[3] **Effective 19 October 2019** In the US Region: A Visa Infinite Business Card Issuer must support a minimum Emergency Cash Disbursement limit of up to USD 5,000 for Stand-In Processing Transactions.

Table 4-7: Provision of Emergency Card Replacements to Cardholders

Card Type	If Cardholder location is within the issuing Visa Region	If Cardholder location is outside the issuing Visa Region
Visa Classic, Visa Electron	Within 1 business day from the time that the Issuer approves the request	Within 3 business days from the time that the Issuer approves the request
Visa Gold/Premier, Visa Rewards, Visa Platinum, Visa Business, Visa Business Electron, Visa Corporate, Visa Purchasing	Within 24 hours from the time that the Issuer approves the request	Within 1 business day from the time that the Issuer approves the

Table 4-7: Provision of Emergency Card Replacements to Cardholders (continued)

Card Type	If Cardholder location is within the issuing Visa Region	If Cardholder location is outside the issuing Visa Region
		request
Visa Infinite (including Visa Infinite Business),[1,2] Visa Signature (including Visa Signature Business), Visa Infinite Privilege,[3] Visa Ultra High Net Worth	Within 24 hours from the time that the Issuer approves the request	Within 24 hours from the time that the Issuer approves the request

[1]   In the US Region: For a Visa Infinite Card, the Issuer must issue a Chip-enabled Emergency Card Replacement if the Issuer or its agent supports Chip technology.

[2]   **Effective 19 October 2019** In the US Region: For a Visa Infinite Business Card, the Emergency Card Replacement must include Card Verification Value (CVV) encoding, and provide a minimum spending limit of up to USD 10,000.

[3]   In the Canada Region: A Visa Infinite Privilege Issuer must issue a Chip-enabled Emergency Card Replacement if the Issuer or Issuer processor is enabled for Chip issuance.

ID# 0002626	Edition: Apr 2020	Last Updated: Apr 2020

4.1.14.3   Requirements for Emergency Service Locations

An Issuer must ensure that its Emergency Service Location complies with all of the following:

- Is able to authorize an Emergency Cash Disbursement if Stand-In Processing Accounts for the Issuer are available and if the Issuer fails to respond as specified in *Section 4.1.14.2, Emergency Cash Disbursement and Emergency Card Replacement Provision Requirements*

- Is available during normal business hours to respond to a request for an Emergency Cash Disbursement or Emergency Card Replacement

- Notifies Visa Global Customer Care Services (within 3 calendar days) that the Cardholder has picked up the Emergency Cash Disbursement or Emergency Card Replacement

ID# 0002631	Edition: Apr 2020	Last Updated: Apr 2019

4.1.14.4   Issuer Provision of Stand-In Processing Accounts for Emergency Cash Disbursements and Emergency Card Replacements

If an Issuer supports Stand-In Processing Accounts for Emergency Cash Disbursements and Emergency Card Replacements, it must provide to Visa Global Customer Care Services, via a secure method, at least 5 activated Stand-In Processing Accounts per BIN.

ID# 0030591	Edition: Apr 2020 | Last Updated: Apr 2019

4.1.14.5   Visa Global Customer Assistance Services Provision Requirements

An Issuer must provide the Visa Global Customer Assistance Services, as follows:

Table 4-8: Provision of Visa Global Customer Assistance Services

Service	Issuer must provide service for:
Cardholder Inquiry Service	All Visa products, except: • Visa Large Purchase Advantage • In the Europe Region: Virtual Accounts
Emergency Cash Disbursement	All Visa products, except:[1] • Virtual Accounts[2] • Visa Agro Cards • Visa Check Cards • Visa Classic Cards • Visa Electron Cards (In the CEMEA Region: Required for Visa Business Electron Cards) • Prepaid Cards (A Visa Corporate Prepaid Card Issuer must have the ability to offer an Emergency Cash Disbursement, if requested.) • Travel Prepaid Cards/Visa TravelMoney (in the LAC Region: required for Visa TravelMoney Student Cards) • In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: Visa Purchasing Cards • In the Europe Region: Visa Gold Cards issued to Prepaid Accounts where full Cardholder due diligence (for example: KYC) has not been completed to the Issuer's satisfaction
Emergency Card Replacement	All Visa products, except:[1] • Virtual Accounts[2] • Visa Classic Cards • Visa Electron Cards

Table 4-8: Provision of Visa Global Customer Assistance Services (continued)

Service	Issuer must provide service for:
	• Visa Large Purchase Advantage • Prepaid Cards
Exception File Updates	As specified in *Section 7.3.5.1, Exception File Updates*
Lost/Stolen Card Reporting	All Cards
¹ The Issuer must provide a response to each Cardholder request for the service.	
² In the AP Region, Canada Region, Europe Region, LAC Region, US Region: Prohibited for Virtual Accounts	

ID# 0004081   **Edition: Apr 2020 | Last Updated: Apr 2020**

4.1.15   Insurance/Benefits

4.1.15.2   Visa Cardholder Benefit Requirements by Product – Canada Region

In the Canada Region: An Issuer must, at minimum, provide the following product-specific Cardholder benefits:

Table 4-9: Cardholder Benefits by Product Type – Canada Region

Product	Auto Rental Collision/Damage Waiver	Legal Referral Assistance and Cash Disbursement	Medical Referral Assistance and Cash Disbursement
Visa	Optional	Optional	Optional
Visa Gold	Optional	Optional	Optional
Visa Platinum	Optional	Optional	Optional
Visa Infinite	Required	Required	Required
Visa Infinite Privilege	Required	Required	Required
Visa Business	Optional	Optional	Optional
Visa Infinite Business	Required	Required	Required
Visa Corporate	Optional	Required	Required

Table 4-9: Cardholder Benefits by Product Type – Canada Region (continued)

Product	Auto Rental Collision/Damage Waiver	Legal Referral Assistance and Cash Disbursement	Medical Referral Assistance and Cash Disbursement
Visa Purchasing	Optional	Not applicable	Not applicable

ID# 0028064   Edition: Apr 2020 | Last Updated: Apr 2017

4.1.15.3   Insurance Program Issuer Requirements – US Region

An Issuer that offers Visa-funded insurance Card benefits must comply with the following requirements:

- Meet all Cardholder notification requirements prescribed by insurance regulators and available at *visacardbenefits@cbsiservices.com*

- Defend and pay a Cardholder for any insurance claim if the Cardholder files a claim based on an insurance certificate or other disclosure of terms, conditions, and exclusions and either of the following:

    - The Issuer failed to send, or cannot provide evidence of having sent, information advising the Cardholder that such coverage was no longer available.

    - The Issuer misrepresented the actual terms of the coverage underwritten, misstated the type or scope of coverage offered by the Issuer, or altered the insurance coverage description without written approval provided by the insurance provider or its appointed designee, and such misrepresentation, misstatement, or alteration results in an obligation or claim to pay a claim that was not otherwise covered.

- If choosing to meet the required minimum benefits for a given product platform via an alternate insurance provider, assume all related expense, operational support, and notification requirements, including the necessary quality assurance and program liability. The Issuer must also notify Visa and provide details as requested by Visa and/or insurance agency to ensure that the minimum requirements are met.

- Pay for an otherwise valid insurance claim if either of the following:

    - The Issuer did not maintain coverage.

    - The insurance carrier would have been responsible but failed to pay a valid claim due to insolvency, bankruptcy, or other financial inability to meet its policy obligations.

- Inform Cardholders that in order to receive benefits their beneficiaries must prove that the Cardholder purchased the product or service with a Card

---

ID# 0000420   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.15.6   Visa Platinum Business and Visa Infinite Business Cardholder Alternative Benefits – Europe Region

Effective 18 July 2020 In the Europe Region: The alternative Cardholder benefits provided by a Visa Platinum Business Card Issuer and a Visa Infinite Business Card Issuer must comply with all of the following:

- Able to be objectively valued, with a clear market value or recommended retail price
- Be an ongoing product feature and not promotional in nature with customer hurdles or eligibility requirements
- Be re-invested into the Card relationship, and not be used to cross-subsidize other products
- Be actively and regularly promoted to Cardholders using all of the following methods:
  - On all advertising or marketing materials for the Card program
  - In the Cardholder communication material included with the Card delivery
  - At least twice per year in all customer-facing channels
- Exclude benefits that are typically provided in campaign acquisition and portfolio management activities (for example: one-off bonus points, fee waivers, or other spend stimulation benefits)

ID# 0030700   Edition: Apr 2020 | Last Updated: New

4.1.16   Preauthorized Payment Cancellation Service

4.1.16.1   Preauthorized Payment Cancellation Service Issuer Participation

Effective through 16 August 2020 in the Europe Region, effective through 18 October 2020 in the AP Region, Canada Region, CEMEA Region, LAC Region, and effective through 16 April 2021 in the US Region An Issuer that participates in the Preauthorized Payment Cancellation Service must do all of the following:

- Correctly specify the type of stop payment order
- Provide complete and accurate information pertaining to the stop payment order
- Keep stop payment order information current in the Cardholder database

---

ID# 0026228   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.16.2   Preauthorized Payment Cancellation Service Limitations

Effective through 16 August 2020 in the Europe Region, effective through 18 October 2020 in the AP Region, Canada Region, CEMEA Region, LAC Region, and effective through 16 April 2021 in the US Region A Member must not disclose information associated with the Preauthorized Payment Cancellation Service other than data relating to the Member's own Cardholder and/or Merchant to any other party unless otherwise authorized by Visa.

ID# 0026229   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.17   Visa Checkout

4.1.17.1   Visa Checkout – Card Enrollment

An Issuer must not restrict a Visa Checkout Account Holder from enrolling the Issuer's Card in one or more Visa Checkout accounts.

ID# 0026989   Edition: Apr 2020 | Last Updated: Oct 2014

4.1.17.2   Visa Checkout – Transaction Requirements

If a Transaction is conducted through Visa Checkout with a Visa-branded product, it is subject to the same requirements as any other Visa Transaction.

ID# 0026988   Edition: Apr 2020 | Last Updated: Oct 2014

4.1.18   Visa Token Service

4.1.18.1   Visa Token Service (VTS) Issuer Participation Requirements

An Issuer that uses the Visa Token Service (VTS) may participate in one or more Token Requestor solutions available through the applicable enrollment process.

The Issuer assumes full responsibility for all of the following:

- Validating Cardholder identity[1]
- Provisioning and maintenance decisions for Tokens
- Compliance with terms and conditions[1]
- Performing life cycle management associated with Tokens and their underlying Payment Credentials[2]

Visa Token Service Basic Issuer Participants[3] will be enrolled by Visa to participate in the VTS for Card-Absent Environment Transactions and must, unless otherwise specified, comply with all rules relating to Tokens and the VTS.

In the Europe Region: An Issuer may choose to opt out of being a Visa Token Service Basic Issuer Participant.

[1] This requirement does not apply to a Visa Token Service Basic Issuer Participant.

[2] This requirement is optional for a Visa Token Service Basic Issuer, except in the CEMEA Region, the Europe Region, and the LAC Region.

[3] Where an Issuer authorizes an Account Verification request from the Visa Token Service, that Authorization represents an instruction to Visa to provision a Token. Visa will not issue a Token on the Issuer's behalf if the Issuer declines an Account Verification request from the Visa Token Service.

ID# 0029515   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.18.2   Visa Token Service – Visa Use of Participating Issuer Data

An Issuer that uses the Visa Token Service agrees and acknowledges that Visa may access, use, store, update, or disclose[1] the Issuer's data, including Issuer data associated with the Issuer's participation in other Visa products, programs, or services, in compliance with applicable laws or regulations to do any of the following in connection with an Issuer's use of Tokens:

- Generate, store, modify, monitor, or provision Tokens and Payment Account References
- Process, support, and resolve customer inquiries or disputes
- Prevent or reduce actual or potential fraud, unauthorized Transactions, claims, or liability
- Manage risk and compliance obligations
- Create and distribute aggregated statistics and reports that do not reveal personally identifiable information
- Comply with any judicial process or government agency having or claiming jurisdiction over Visa
- Provide information to a Token Requestor to enable the Token Requestor to do any of the following:
  - Obtain a Token for use in connection with the Token Requestor's payment solution
  - Provide Transaction alerts to the Cardholder
  - Provide Transaction history to the Cardholder
  - Deliver reporting to a Token Requestor

[1] Includes disclosure to Visa employees, subsidiaries, affiliates, counsel, and agents as necessary

---

ID# 0029516   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.18.3   Visa Token Service – Issuer Use of Token Requestor Data

Unless bilateral agreements are in place between a Token Requestor and an Issuer, an Issuer that participates in the Visa Token Service and receives Token Requestor data in connection with the Visa Token Service may use such data to perform the following activities:

- Provide customer service support and manage or resolve disputes
- Support operational functions including accounting, billing, auditing, and collection
- Create, use, or distribute aggregated statistics and reports that do not reveal personally identifiable Cardholder information
- Develop, manage, and enhance fraud prevention and risk mitigation strategies for Token provisioning
- Comply with any judicial or government-mandated processes
- Protect or exercise any legal rights afforded by law

The Issuer must not:

- Sell or resell the Token Requestor data
- Isolate raw Token Requestor data for any purpose
- Reformulate aggregated data to establish any identifiable association between the data and Visa Token Service participants

ID# 0029517   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.18.4   Token Transaction Processing Requirements – Europe Region

In the Europe Region: If a Transaction is initiated with a Token, the Transaction must be submitted for Online Authorization.

Visa reserves the right to decline, on an Issuer's behalf, a Transaction initiated with a Token if the Token does not comply with domain control requirements specified in the *EMV Payment Tokenization Specification.*

ID# 0029817   Edition: Apr 2020 | Last Updated: Apr 2018

4.1.18.5   Visa Token Service Issuer Requirements – Europe Region

In the Europe Region: To participate in the Visa Token Service, an Issuer must register with Visa and ensure that no third-party Token Service Provider associates a payment Token with an Account Number in an Account Range assigned to the Visa Token Service.

If an Issuer chooses to act as a Token Requestor for Cards it has not issued, the Issuer must engage with Visa as a third-party Token Requestor.

ID# 0029868	Edition: Apr 2020	Last Updated: Apr 2020

4.1.18.6   Host Card Emulation and Secure Element Third-Party Wallet Token Requirements – Europe Region

In the Europe Region: An Issuer that engages with a third-party wallet Token Requestor for a host card emulation (HCE) or secure element Token service must do all of the following:

- Notify Visa of the Visa-approved third-party Token Requestor with which the Issuer intends to engage
- Implement an engagement and testing period, the duration of which will be agreed on a case-by-case basis by the Issuer, third-party Token Requestor, and Visa
- Provide call center and customer service support
- Comply with provisioning requirements, as specified in *Section 4.1.18.5, Visa Token Service Issuer Requirements – Europe Region*
- Agree that a Token Requestor that is enrolled in the Delegated Authentication Program will provide strong customer authentication, on the Issuer's behalf, in line with the Delegated Authentication Program.

ID# 0030556	Edition: Apr 2020	Last Updated: Apr 2019

4.1.18.7   Issuer Mobile Application Token Requirements – Europe Region

In the Europe Region: An Issuer that acts as a Token Requestor through a mobile payment application deployed by the Issuer must submit the proposed application to Visa for approval.

Visa reserves the right to withdraw approval of a mobile payment application at any time if Visa determines that the application does not comply with Visa requirements and payment industry standards.

ID# 0030557	Edition: Apr 2020	Last Updated: Apr 2018

4.1.18.8   Use of Issuer Card Artwork in Tokenization Services – Europe Region

In the Europe Region: An Issuer must provide Visa with its Card artwork and consent to Visa sharing the Card artwork with all of the following:

- A third-party Token Requestor for use in that Token Requestor's mobile application
- A Stored Credential Token Requestor for use on its payment screen and all screens that show account information
- A Merchant, where Visa provides that Merchant with a payment Token

Where an Issuer does not supply its Card artwork, Visa will provide default Card artwork to all of the above entities.

| ID# 0030558 | Edition: Apr 2020 | Last Updated: Apr 2018 |

4.1.19   Chip Issuance Requirements

4.1.19.2   Contact Chip and Contactless Issuer Requirement for Cryptogram Version Number

Effective 17 October 2020[1] An Issuer must ensure that a contact Chip or Contactless Card issued or reissued on or after 17 October 2020 is not personalized to support Cryptogram version number (CVN) 10 or 17, or proprietary CVNs that use a static key in the calculation.

[1]   **Effective 17 August 2021** For the AP Region (Japan)

| ID# 0030131 | Edition: Apr 2020 | Last Updated: Apr 2018 |

4.1.19.3   Chip Card Issuing Requirements – AP Region (Australia, New Zealand)

In the AP Region: All of the following must be EMV-Compliant and VIS-Compliant:

- In Australia and New Zealand: All Reloadable Prepaid Cards (except Visa TravelMoney Cards)
- In New Zealand: All Debit Cards

| ID# 0026145 | Edition: Apr 2020 | Last Updated: Apr 2020 |

4.1.19.4   Cash-Back Services on Visa Debit Chip Cards – AP Region (Australia)

In the AP Region (Australia): An Issuer must offer Cash-Back services on its Debit Cards issued as Chip Cards.

ID# 0026153	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.5   Chip Card Issuing Requirement – AP Region (India)

In the AP Region (India): An Issuer must be capable of issuing EMV-compliant Cards.

All Magnetic-Stripe Debit Cards and Credit Cards that have been used internationally must be reissued as EMV Chip Cards with PIN as the preferred Cardholder Verification Method (CVM).

ID# 0027955	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.6   Chip Card Account Requirements

An Issuer of a Chip Card must do all of the following:

- Not use a Visa Smart Payment application to directly credit or debit any account other than an account that is maintained by that Issuer or another Member under contract with the Issuer
- Allow a Cardholder to select the service and account to be used for a Transaction, as permitted by applicable laws or regulations
- Designate a Payment Credential for each account accessed by a Visa Smart Payment application
- Specify an alphanumeric name for each funding account facilitated by the Visa Smart Payment application when the Chip provides access to more than one account
- In the Europe Region: In addition, notify Visa of all Payment Applications contained in the Chip. Visa reserves the right to review and approve or prohibit the use of Payment Applications on Visa Cards or for Visa services.

ID# 0004031	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.7   Visa Chip Card Payment Application

A Chip Card bearing a Visa-Owned Mark must be capable of facilitating the Payment Application associated with that Mark.

The Payment Application on all Visa or Visa Electron contact Chip Cards must be VIS-Compliant.

ID# 0003613	Edition: Apr 2020 | Last Updated: Apr 2016

4.1.19.8   Appropriate Marks on Chip Cards

A Card containing a Chip must bear the appropriate Mark for the Visa or Visa Electron Payment Application facilitated by the Chip.

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

ID# 0003612	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.9   Non-Visa Services Facilitated by Chip Cards

A Chip Card may facilitate access to non-Visa services only if all of the following requirements are met:

- Services do not compromise the security or functional integrity of the Visa Smart Payment Applications.
- Additions of these services are managed and controlled by the Issuer or its Sponsored Member.
- The Issuer Indemnifies Visa for and against Claims and Liabilities arising out of or in connection with non-Visa services facilitated by the Chip Card.

Visa may review and approve all applications contained in a Chip used to facilitate a Visa payment.

ID# 0003598	Edition: Apr 2020 | Last Updated: Apr 2018

4.1.19.10 Contactless Issuer Requirements

A Contactless Payment Device Issuer must comply with the following:

Table 4-10: Contactless Payment Device Issuer Requirements

Applies to Contactless Payment Devices issued or replaced on or after:	Region/Country	Required VCPS Version	Support for qVSDC Transaction Path	Support for MSD Transaction Path	Form Factor Indicator
1 January 2012	AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region	2.0 or later	Required	Optional	N/A
1 January 2012	US Region	Any	Optional	Required	N/A
1 April 2015	AP Region (excluding Japan), CEMEA Region	2.1 or later	Required	Not permitted, except for Mobile Payment Devices	Required

---

Table 4-10: Contactless Payment Device Issuer Requirements (continued)

Applies to Contactless Payment Devices issued or replaced on or after:	Region/Country	Required VCPS Version	Support for qVSDC Transaction Path	Support for MSD Transaction Path	Form Factor Indicator
	(excluding Bahrain, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, United Arab Emirates)				
1 April 2015	AP Region (Japan)	2.1 or later	Required	Not permitted, except: • Optional for Mobile Payment Devices • Optional for Issuers that issued a Contactless Payment Device before 1 April 2015	Required
1 July 2015	CEMEA Region	2.1 or later	Required	Not permitted, except for Mobile Payment Devices	Required
1 October 2015	AP Region, CEMEA Region, Europe Region, LAC Region	2.1 or later	Required	Not permitted, except for Mobile Payment Devices	Required
1 October 2015	Canada Region,	2.1 or later	Required	Optional	Required

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

Table 4-10: Contactless Payment Device Issuer Requirements (continued)

Applies to Contactless Payment Devices issued or replaced on or after:	Region/Country	Required VCPS Version	Support for qVSDC Transaction Path	Support for MSD Transaction Path	Form Factor Indicator
	US Region				
31 December 2015	Canada Region	2.1 or later	Required	Not permitted for any device personalized with a Token	Required

In the Europe Region: A Contactless Payment Device Issuer must be certified by Visa for the Authorization, Clearing, and Settlement of Contactless payments and must comply with the following:

Table 4-11: Contactless Payment Device Issuer Requirements – Europe Region

Applies to:	Required VCPS Version	Support for qVSDC Transaction Path	Support for MSD Transaction Path	Form Factor Indicator
All Contactless Payment Devices (except Mobile Payment Devices)	2.1	Required	Not permitted[1]	Required
All Contactless Payment Devices (except Mobile Payment Devices) that are Prepaid Cards	2.1.1	Required	Not permitted[1]	Required
All Contactless Payment Devices with an X2X Service Code	2.1.1 or later	Required	Not permitted[1]	Required
[1] In the Europe Region: An Issuer must decline any Authorization Request using the Contactless MSD transaction path				

4.1.19.11   Visa Contactless Authentication Issuer Requirement

A Contactless Chip Card issued on or after 13 April 2019 must support offline data authentication with Online Authorization using fast Dynamic Data Authentication, as specified in *Visa Contactless Payment Specification* version 2.1 and later.

This does not apply to:

- In the Europe Region: A payment solution that uses a cloud-based payments Mobile Application, unless it is to be used for a Mass Transit Transaction

- In the US Region: A Contactless Chip Card

ID# 0029157   Edition: Apr 2020 | Last Updated: Apr 2018

4.1.19.12   Notification of Contactless Payment Device Risks and Restrictions

An Issuer that provides a Contactless Payment Device to a Cardholder must provide, before or at the time of issuance, written notification that informs the Cardholder of potential risks and restrictions associated with the Contactless Payment Device, including, but not limited to, the following:

- The inability to use the Contactless Payment Device at an Acceptance Device where Card insertion is required

- Any daily Transaction amount limit implemented by the Issuer in connection with the Contactless Payment Device, if applicable

- For a Contactless Payment Device in the form of an adhesive Visa Micro Tag, the risk of impairing the functionality of a mobile phone or other device to which a Contactless Payment Device is attached

- For a Contactless Payment Device in the form of an adhesive Visa Micro Tag, the risk of invalidating the manufacturer's warranty, if applicable, for a mobile phone or other device to which Contactless Payment capability is attached

ID# 0026159   Edition: Apr 2020 | Last Updated: Oct 2015

4.1.19.13   Contactless Payment Device Requirements

An Issuer that issues a Contactless Payment Device must ensure that the Contactless Payment Device complies with all of the following:

- Is linked to a valid, unexpired Card account,[1] excluding Prepaid Cards (a Contactless Payment Device may be assigned a different Payment Credential)[2]

- Is issued with a PIN for use at ATMs, if the Issuer supports Contactless ATM Transactions

- In the AP Region, CEMEA Region: If issued on or after 1 April 2015,[3] both:

  – Is personalized with the application program ID

  – Supports offline data authentication for Online Authorization

[1] If the Contactless Payment Device is not a physical Card, the linked account must also have a standard Card issued to it (except if the Contactless Payment Device is a Prepaid Card).

[2] In the AP Region (South Korea): This does not apply.

[3] In the CEMEA Region (Bahrain, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, United Arab Emirates): 1 July 2015

ID# 0002052	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.16 Cardholder Verification Method Preferences

A Chip Card Issuer must ensure that the Cardholder Verification Method (CVM) preferences are communicated by the Chip Cardholder Verification Method list to the Chip-Reading Device at the Point-of-Transaction.

The Issuer of a Chip Card bearing a Payment Application must comply with *4.1.19.16, Cardholder Verification Method Preferences*. This does not apply to Mobile Payment Devices.

In the AP Region, CEMEA Region: A Contactless Payment Device must include a Cardholder Verification Method to facilitate Contactless Payment Transactions, as follows:

Table 4-12: CVM Requirements for Contactless Payment Devices – AP Region and CEMEA Region

Region/Country	Applies to Contactless Payment Devices issued on or after:
AP Region	1 April 2015
CEMEA Region (excluding Bahrain, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, United Arab Emirates)	1 April 2015
CEMEA Region (Bahrain, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, United Arab Emirates)	1 July 2015

ID# 0008186	Edition: Apr 2020 | Last Updated: Oct 2017

4.1.19.17   Cardholder Verification Method List – Canada Region

In the Canada Region: An Issuer of a Compliant Chip Card must ensure that all of the following requirements are met:

- The compliant Chip Card contains a Cardholder Verification Method (CVM) list, with at minimum, the following methods of Cardholder verification:
  - "Offline PIN at POS"
  - "Online PIN at ATM"
  - "Signature"
  - "No CVM required"
- Use of CVM condition codes relating to cash or Cash-Back do not prevent the completion of Manual Cash Disbursements.
- The CVM "Offline PIN at POS" is activated and is the preferred CVM unless either the:
  - Compliant Chip Card was issued no more than 6 months before the date of the Compliant Chip Card Transaction in question
  - Cardholder is subject to a disability or impairment that would prevent PIN use

ID# 0008187	Edition: Apr 2020 | Last Updated: Oct 2015

4.1.19.19   Additional Cardholder Authentication for Token Issuance – Canada Region

In the Canada Region: When an Issuer requires additional Cardholder authentication before provisioning a payment Token to a third-party wallet, the Issuer must implement at least 2 additional Cardholder authentication methods.

ID# 0029456	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.21   Card Verification Value Requirements

An Issuer must be capable of receiving the POS Entry Mode code and, for Magnetic-Stripe Transactions, processing the Card Verification Value.[1]

All EMV Chip Cards issued on or after 1 January 2009 must use Chip Card Verification Value-iCVV as part of the Magnetic-Stripe Image.

[1]   An Issuer may verify the CVV itself, or may use VisaNet or its processor.

ID# 0008133	Edition: Apr 2020 | Last Updated: Oct 2017

4.1.19.22   Chip Card Authentication

All Chip Card Issuers must perform, and be capable of acting on the results of, validation of EMV Online Card Authentication Cryptograms for all Chip-initiated Authorization messages processed through VisaNet. Online Card Authentication support may be provided by the Issuer directly, or through either:

- VisaNet
- Third party/VisaNet Processor or Visa Scheme Processor

ID# 0007163	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.23   Parameters to Enable Offline Chip Authorization

An Issuer of the following Chip Cards must define parameters to enable Offline Chip Authorization:

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Chip Card containing a Visa Smart Payment Application with Offline Authorization controls
- In the Europe Region: A Visa or Visa Electron Chip Card

An Issuer may exempt a Visa Card encoded with X Service Code from this requirement. In the Europe Region: In addition, an Issuer may exempt Visa Purchasing Cards from this requirement.

ID# 0004392	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.24   Consecutive Offline Chip Authorization Counters

When Offline Authorization controls are defined in a Chip and the upper limit for consecutive offline counters is specified, all Chip-initiated Transactions must go Online if the upper limit for the total number or value of consecutive offline Transactions is exceeded. If the terminal is unable to go Online, the Transaction must be declined.

ID# 0004393	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.25   Consecutive Offline Chip Authorization Counters Requirement – AP Region

In the AP Region: An Issuer must ensure a domestic Contactless Transaction is authorized online if the cumulative value of consecutive domestic Contactless Transactions authorized offline exceeds the following limits:

Table 4-13: Domestic Contactless Transaction Offline Authorization Limits – AP Region

Country/Territory	Cumulative Offline Limits
Hong Kong	HKD 1,000
Indonesia	IDR 500,000
Japan	JPY 50,000
Malaysia	MYR 400
Philippines	PHP 5,000
Singapore	SGD 200
Taiwan	NTD 10,000
Thailand	THB 4,500

ID# 0029282   Edition: Apr 2020 | Last Updated: Apr 2016

4.1.19.26   Cardholder Name on Chip

For all Contactless Payment Devices issued on after 1 October 2015,[1,2] an Issuer must ensure that the Cardholder name is either:

- Not personalized to be accessible via the contactless interface in the Chip

- Encoded with a generic identifier so that the actual Cardholder name is not transmitted through a Contactless Transaction

[1] In the AP Region, CEMEA Region: 1 April 2015

[2] In the CEMEA Region (Bahrain, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, and United Arab Emirates): 1 July 2015

ID# 0003595   Edition: Apr 2020 | Last Updated: Apr 2016

4.1.19.27   Service Codes on Chip Cards

An Issuer must use a Service Code X on all EMV-Compliant and VIS-Compliant Chip Cards bearing the Visa Brand Mark, Visa Brand Mark with the Electron Identifier, or Plus Symbol.

ID# 0003593   Edition: Apr 2020 | Last Updated: Oct 2016

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

4.1.19.28 Effective Date and Expiration Date Consistency

The expiration date contained in the Chip must be the same as the expiration date encoded on the Magnetic Stripe and on the Card (if displayed). If applicable, the expiration date of proprietary services on the Card must not exceed the Visa or Visa Electron Payment Application expiration date.

The expiration date on a Visa Card, Visa Electron Card, or Card bearing the Plus Symbol must not be later than the expiration date of the Issuer's Public Key, or any security feature containing an expiration date in a Chip, if one is present on the Card.

If an application effective date on a Chip Card is provided within the Chip, it must reflect the same month as the "VALID FROM" date displayed on the Card, if such a date appears on the Card.

For Chip Card products approved by Visa on or after 1 January 2016, an Issuer must ensure that the expiration date contained in the Chip, encoded on the Magnetic Stripe and, if applicable, printed on the Card does not extend beyond the date the product is scheduled to be removed from the list of Visa-approved Chip products.

Visa reserves the right to remove a Chip product from the list earlier than the scheduled date if it discovers a significant security flaw with the associated Chip.

ID# 0003209	Edition: Apr 2020	Last Updated: Oct 2019

4.1.19.29 Integrated Circuit Card Verification Value (iCVV) Requirements – AP Region

In the AP Region: A Chip Card Issuer must certify support for the Integrated Circuit Card Verification Value (iCVV) in the Magnetic Stripe data encoded on the Chip.

The Card Verification Value (CVV) encoded on other (non-Magnetic Stripe) technologies must differ from the CVV encoded on the physical Magnetic Stripe.

ID# 0004087	Edition: Apr 2020	Last Updated: Oct 2014

4.1.19.30 Issuer Requirements for Post-Issuance Updates

Post-Issuance Updates, or new application loading to a Chip containing a Visa or Visa Electron Payment Application must not adversely impact the Transaction completion time at an Acceptance Device or an ATM.

Post-Issuance Updates to add an application or a service to a Visa or Visa Electron Payment Application is not permitted unless the Card bears the appropriate Visa Brand Mark or Visa Brand Mark with the Electron Identifier.

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

Post-Issuance Updates to load an application or a service to a proprietary ATM application that supports Plus requires the addition of the Plus Symbol at the time of Card reissuance. Card reissuance must occur within 5 years of loading the application or service.

ID# 0004035	Edition: Apr 2020	Last Updated: Oct 2016

4.1.19.31 Issuer Control of Post-Issuance Updates

Post-Issuance Updates to a Chip Card containing a Visa or Visa Electron Payment Application must be controlled exclusively by the Issuer.

ID# 0004034	Edition: Apr 2020	Last Updated: Oct 2014

4.1.19.32 Mobile Gateways – Issuer Requirements

An Issuer that uses a mobile gateway for its Mobile Payment Devices must ensure that the mobile gateway is approved by Visa.

ID# 0026796	Edition: Apr 2020	Last Updated: Oct 2014

4.1.19.33 Mobile Payment Devices – Cardholder Verification Method Requirements

An Issuer of a Mobile Payment Device must ensure that the Mobile Payment Device[1] supports a Consumer Device Cardholder Verification Method (CDCVM).

In the AP Region, CEMEA Region, US Region: An Issuer of a Mobile Payment Device must ensure that the Mobile Payment Device supports signature as a Cardholder Verification Method.

In the AP Region: Mobile Payment Devices that facilitate QR code Transactions must support CDCVM as the only Cardholder Verification Method.

[1] Except a Visa Micro Tag

ID# 0026784	Edition: Apr 2020	Last Updated: Oct 2019

4.1.19.34 Mobile Payment Devices – Issuer Requirements

An Issuer of a Mobile Payment Device must both:

- Register with Visa
- Ensure that the Mobile Payment Device is approved by Visa

An Issuer may use any of the following:

- A Visa-approved secure element and a Visa-approved Visa Mobile Payment Application

- A Visa-approved cloud-based payments Visa Mobile Payment Application

- In the AP Region: An Issuer may use a QR code.

If an Issuer pre-sets a Consumer Device Cardholder Verification Method (CDCVM) on the Mobile Payment Device, it must not use a CDCVM that is the same as, or otherwise represents, the PIN on the account if the PIN may also be used with the corresponding standard Card.

An Issuer must not systematically synchronize the Online PIN and the CDCVM on a Mobile Payment Device if the Online PIN is also linked to the corresponding standard Card.

If an Issuer that provides access to a mobile wallet (or an entity acting on the Issuer's behalf to provide access to a mobile wallet solution) uses a secure element and a Visa Mobile Payment Application deployed on or after 1 June 2015, the expiration date of the mobile payment account set by the Issuer or the entity acting on its behalf must not exceed 10 years[1] from the EMVCo Integrated Circuit Certificate Number (ICCN) approval date, if known.

If the ICCN approval date is not known, the expiration date of the mobile payment account must not exceed 3 years from the date of provisioning of the account.

[1] In the AP Region (Japan): The expiration date of the account must not exceed 5 years.

ID# 0026783	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.35   Smart Payment Application Options

An Issuer must define the Payment Application options for its Visa Smart Payment program.

ID# 0004024	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.36   Issuer Use of Visa Public Keys

An Issuer must ensure that the Visa Public Keys used for a Visa or Visa Electron Payment Application are used solely for that purpose.

ID# 0004025	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.37   Chip Card Issuer Terminal Risk Management

A Chip Card Issuer must not inhibit Terminal Risk Management (for example: by programming the Chip to bypass Terminal Risk Management).

ID# 0004026	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.38   Dynamic Data Authentication (DDA) Issuer Requirement

All Chip Cards that do not have contactless functionality and that support offline Authorization must both:

- Support DDA[1] (support for combined DDA/application cryptogram generation remains optional)

- Not support static data authentication[2]

[1] Online-only Chip Cards that do not have contactless functionality or any type of offline data authentication are still permitted.

[2] In the AP Region (Japan): **Effective 1 October 2023**

ID# 0029158	Edition: Apr 2020 | Last Updated: Apr 2016

4.1.19.39   Visa Contactless Application Requirement – AP Region (Australia, Malaysia) and US Regions

In the AP Region (Australia, Malaysia), US Region: An Issuer that issues a Visa Card with contactless payment capability must enable the Visa Contactless Application on the Card.

In the AP Region (Australia): An Issuer must also do both of the following for a Visa Card with multiple contactless payment applications:

- Designate and retain the Visa Contactless Application as the highest priority application

- Not modify the priority of the Visa Contactless Application after issuance

ID# 0027793	Edition: Apr 2020 | Last Updated: Apr 2018

4.1.19.40   PIN as Cardholder Verification Method – Issuer Requirements – AP Region (Australia, New Zealand)

In the AP Region (Australia, New Zealand): All newly issued or reissued Cards must be issued with a PIN as the preferred Cardholder Verification Method (CVM).[1]

In the AP Region (Australia): When PIN bypass is performed for a domestic Chip-initiated Transaction that requires a PIN, the Authorization Request must be declined. This does not apply to an Unattended Transaction.

In the AP Region (New Zealand): When PIN bypass is performed for a domestic Chip-initiated Transaction, the Authorization Request must be declined. This requirement does not apply to an Unattended Transaction.

[1] This does not apply to non-PIN-preferring Cards issued to accommodate specific individual Cardholder needs, as required

by applicable laws or regulations.

ID# 0026146	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.41   Chip Card Application Selection Flag – Canada Region

In the Canada Region: An Issuer may only program an Application Selection Flag (ASF) as follows:

- Where a Compliant Chip Card displays any Visa Brand Name and a competitor brand, the Issuer of that Compliant Chip Card may program an ASF to suppress the ability of the Visa Smart Payment Application contained in the Compliant Chip Card to transact at domestic ATMs.

- Where a Compliant Chip Card displays any Plus Program Mark, the Issuer of that Compliant Chip Card may program an ASF to suppress the ability of the Visa Smart Payment Application contained in the Compliant Chip Card to transact at domestic POS and ATM locations.

ID# 0008733	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.42   Chip Card Online/Offline Data Authentication – Canada and Europe Regions

The following must instruct the terminal to go Online if offline data authentication fails:

- In the Canada Region: A Compliant Chip Card
- In the Europe Region: The Payment Application

If the terminal is unable to go Online, the Transaction must be declined.

ID# 0004626	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.43   Chip Card Script Message Length – Canada Region

In the Canada Region: An Issuer of a Compliant Chip Card must ensure that the length of any script message sent to any of its Compliant Chip Cards does not exceed 128 bytes per Transaction.

ID# 0004631	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.45   Chip Card Issuing Requirements – Europe Region (Liechtenstein, Switzerland)

In the Europe Region (Liechtenstein, Switzerland): An Issuer may issue Cards using card applications that comply with at a minimum the EMVI'16 specifications only if the Issuer satisfies the Visa approval requirements for the use of the EMVI'16 specifications.

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

ID# 0030008   Edition: Apr 2020 | Last Updated: Oct 2017

4.1.19.46   Chip Card Issuing Requirements – Europe Region (Germany, Luxembourg)

In the Europe Region (Germany, Luxembourg): An Issuer may issue Cards using card applications that comply with the SECCOS specifications only if the Issuer satisfies the Visa approval requirements for the use of the SECCOS specifications.

ID# 0030010   Edition: Apr 2020 | Last Updated: Oct 2017

4.1.19.47   Identification of a Chip Card – Europe Region

In the Europe Region: A Chip Card Issuer must ensure that the Issuer is designated and identified to a Cardholder as the Issuer of that Cardholder's Chip Card. Only one Issuer may be identified to the Cardholder in relation to each Chip Card.

ID# 0029619   Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.48   Visa Smart Debit/Credit Personalization Assistant – Europe Region

In the Europe Region: For a new and/or modified Chip Card program, an Issuer must submit to Visa both:

- A Card profile for validation using the Visa Smart Debit/Credit Personalization Assistant Tool
- **Effective through 24 January 2020** A personalized Card showing that the production Card matches the Visa Smart Debit/Credit Personalization Assistant Profile submitted to, and approved by, Visa. The personalized Card may contain either test keys or production keys and may be used for Issuer host certification.
- **Effective 25 January 2020** A personalized Card showing that the production Card matches the Visa Smart Debit/Credit Personalization Assistant Profile submitted to and approved by Visa, or, if the self-service option is selected, a pass report from a qualified test tool. The personalized Card may contain either test keys or production keys and may be used for Issuer host certification.

ID# 0029620   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.49   Contactless Payment Device Issuance Requirements – AP, CEMEA, Europe, and LAC Regions

In the AP Region, CEMEA Region, Europe Region, LAC Region: An Issuer must comply with all of the following:

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

Table 4-14: Contactless Payment Device Issuance Requirements – AP Region, CEMEA Region, Europe Region, and LAC Region

Issuer Region/Country	Requirements
AP Region	
All countries	A Chip Card issued on or after 13 October 2018 must have Contactless capability. This does not apply to a Non-Reloadable Prepaid Card.
CEMEA Region	
All countries	A Card issued on or after 13 April 2019 must have Contactless capability. This does not apply to a Non-Reloadable Prepaid Card.
Europe Region	
Andorra, Austria, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Gibraltar, Greece, Greenland, Hungary, Iceland, Liechtenstein, Luxembourg, Netherlands, Poland, Republic of Ireland, Romania, Slovakia, Slovenia, Spain, Switzerland, United Kingdom, Vatican City **Effective 25 January 2020** Belgium, Estonia, Latvia, Lithuania, Malta, Monaco, Norway, Portugal, San Marino, Sweden **Effective 23 January 2021** Israel, Turkey	A new or replacement Card must have Contactless capability or be issued in conjunction with a Visa Micro Tag or a Mobile Payment Device. This does not apply to: • A Prepaid Card • A Visa Purchasing Card • A Card that requests Online Authorization for every Transaction • An ATM access-only Card that is not used at a Point-of-Transaction Acceptance Device • A Card issued to a Cardholder that chooses to opt out of being issued a Contactless Payment Device

Italy	• A new or replacement Card must have Contactless capability. This does not apply to:
	  – An ATM access-only Card that is not used at a Point-of-Transaction Acceptance Device
	  – A Card issued to a Cardholder that chooses to opt out of being issued a Contactless Payment Device

Table 4-14: Contactless Payment Device Issuance Requirements – AP Region, CEMEA Region, Europe Region, and LAC Region (continued)

Issuer Region/Country	Requirements
	• **Effective 15 April 2023** All Cards must have Contactless capability.
LAC Region	
All countries	A Card issued on or after 13 October 2018 must have Contactless capability. This does not apply to a Non-Reloadable Prepaid Card.

ID# 0029813   Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.50   Issuer Liability for Visa Smart Payment – Europe Region

In the Europe Region: An Issuer is responsible for setting the parameter values and processing options contained in a Visa Smart Payment application, and any loss resulting from such parameter values and processing options will be borne by the Issuer.

ID# 0029594   Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.51   Integrated Circuit Card Verification Value (iCVV) Requirements – Europe Region

In the Europe Region: All EMV-Compliant Chip Cards must use the Integrated Card Verification Value (iCVV) in the Magnetic Stripe data encoded on the Chip.

ID# 0029797   Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.52   Chip Authorization Requirements – Europe Region

In the Europe Region: For an Authorization of a Chip Transaction that is below the Floor Limit, an Issuer must ensure that the controls contained in each Chip are capable of both:

• Instructing the Acceptance Device to go Online

• Approving the Chip Transaction offline

ID# 0029832   Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.53 Application Identifier Priority – US Region

In the US Region: A Visa-owned Application Identifier must always be the highest priority Application Identifier personalized on a VSDC Applet,[1] including in situations where the Visa Rules permit the personalization of non-Visa Application Identifiers on a VSDC applet.

When both the Visa Application Identifier and the Visa US Common Debit Application Identifier are personalized on a VSDC applet, the Visa Application Identifier must be the highest priority Application Identifier.

[1] This does not apply to the Visa US Common Debit Application Identifier when personalized on a non-Visa Card.

ID# 0027578	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.54 Contact and Contactless Chip Application Transaction Counter (ATC)

An Issuer must not decline a Transaction solely on the basis that the Application Transaction Counter (ATC) is out of sequence.

In the US Region: An Issuer must validate the ATC on each of its Cards with Magnetic-Stripe Data contactless payment capability during the Authorization process for a Contactless Transaction.

ID# 0002064	Edition: Apr 2020 | Last Updated: Oct 2018

4.1.19.55 Visa-Owned Chip Technology Use

Visa-owned Chip technology must be used solely for the purpose of facilitating a Visa Transaction, Interlink transaction, Visa Electron Transaction, or Plus Transaction.[1] Any other use requires the prior written permission of Visa.

Visa-owned Chip technology includes, but is not limited to, all of the following:

- Visa Integrated Circuit Card Specification
- Visa Smart Debit/Credit (VSDC) applet
- Visa Contactless Payment Specification
- Visa Mobile Contactless Payment Specification
- Visa Cloud-Based Payments Contactless Specification
- Visa Mobile Payment Application
- Visa, Interlink, Visa Electron, and Plus Payment Application Identifiers

[1] In the US Region, US Territory: This does not apply to a transaction initiated using the Visa US Common Debit Application

Identifier from a US Covered Visa Debit Card personalized in accordance with the US common debit personalization requirements or a transaction initiated as specified in the *Plus System, Inc. Operating Regulations* or *Interlink Core Rules and Interlink Product and Service Rules*

ID# 0027577	Edition: Apr 2020 | Last Updated: Apr 2017

4.1.19.56 Visa Micro Tag Issuance Requirements

An Issuer may issue a Visa Micro Tag only if a Cardholder either:

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Already possesses a corresponding full-size Card
- Is issued a corresponding full-size Card at the same time as the Visa Micro Tag

The Visa Micro Tag and the corresponding full-size Card must be the same Visa product type and offer the same benefits.

This does not apply to Prepaid Cards that are Contactless Payment Devices.

ID# 0027966	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.19.57 Chip Interoperability Compliance Program

Visa requires the implementation of the Chip Interoperability Compliance Program when Visa determines that progress toward an agreed resolution is no longer acceptable.

ID# 0001291	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.58 EMV Liability Shift – Issuer Liability for Card-Present Counterfeit Chip Card Transactions

A Counterfeit Card Transaction completed in a Card-Present Environment is the liability of the Issuer if both:

- The Transaction takes place at an EMV-Compliant Chip-Reading Device.
- If the Transaction is Chip-initiated, it is correctly processed, and, if authorized Online, the Authorization Request includes Full-Chip Data.

In the Europe Region: In addition, a Counterfeit Card Transaction completed in a Card-Present Environment is the liability of the Issuer if all of the following apply:

- The Transaction does not take place at a Chip-Reading Device that complies with the *Transaction Acceptance Device Requirements*, and is not a Fallback Transaction completed following correct acceptance procedures.

- The Card is a Chip Card containing a Visa Smart Payment.

- If Online Authorization was obtained, the Authorization record indicates that either CVV verification was not performed or that the CVV failed verification.

ID# 0001820	Edition: Apr 2020 | Last Updated: Oct 2016

4.1.19.59   EMV Liability Shift – Issuer Liability for Non-Counterfeit Card-Present Fraudulent Transactions

A non-Counterfeit Card fraudulent Transaction completed in a Card-Present Environment is the liability of the Issuer if all of the following occur:

- The Transaction takes place at an EMV PIN-Compliant Device.

- Correct acceptance procedures have been followed (including obtaining Online approval for Transaction amounts over the applicable maximum authorized Floor Limit).

- The Transaction is Chip-initiated and correctly processed to completion and, if authorized Online, the Authorization Request includes Full-Chip Data.

ID# 0001834	Edition: Apr 2020 | Last Updated: Apr 2015

4.1.19.60   Liability for Chip Fallback Transactions

A Transaction accepted as a Fallback Transaction is the liability of the Issuer if all of the following apply:

- The Transaction is authorized by the Issuer or the Issuer's agent.

- Appropriate values identifying the Transaction as a Fallback Transaction are included within the related Authorization Message.

- Correct acceptance procedures are followed.

ID# 0001835	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.19.61   Liability for Chip-Initiated Offline-Authorized Transactions

The Issuer is liable for a Chip-initiated, offline-authorized Transaction if all of the following apply:

- Terminal Risk Management is performed.
- Merchant's Floor Limit is not exceeded.

ID# 0004039	Edition: Apr 2020 | Last Updated: Apr 2015

4.1.19.62   Liability in Card-Present Environment – Canada Region

In the Canada Region: An Issuer is liable for a Transaction in a Card-Present Environment, whether or not the Transaction is Chip-initiated, when both the:

- Transaction takes place at a Compliant Chip Card Reading Device with a Compliant PIN entry device within Canada
- The Acquirer has complied with all Card acceptance requirements

ID# 0004962	Edition: Apr 2020 | Last Updated: Oct 2014

4.1.20   Pass-Through Digital Wallet Requirements

4.1.20.1   Pass-Through Digital Wallet Requirements

For a Pass-Through Digital Wallet, a Digital Wallet Operator (DWO) must:

- At the time of loading the Cardholder information in the Pass-Through Digital Wallet, obtain written Cardholder consent to all of the following:
  - Use of the stored account information to initiate Transactions
  - The purpose for which the Cardholder's information will be used
  - The expiration date of the agreement, if applicable
- Not contract with another DWO to provide payment services
- Display on the payment screen and all screens that show Account information both:
  - The last 4 digits of the Payment Credential
  - The Visa Brand Mark or the name "Visa" in text immediately next to a Visa payment option

ID# 0029534	Edition: Apr 2020 | Last Updated: Apr 2020

4.1.21   Payment Solution Providers

4.1.21.1   Issuer Requirements for Bill Payment Providers – US Region

Effective 18 April 2020 In the US Region: An Issuer that contracts with a Bill Payment Provider[1] (BPP) must do all of the following:

- Register the BPP with Visa and obtain written approval for each BPP before the BPP makes any payments as a BPP

- If the BPP plans to expand or introduce an additional service or product type than what was originally approved by Visa, the BPP must register and obtain further approval for every new service or product type

- Certify that the BPP qualifies as a BPP

- Conduct an adequate due diligence review of the BPP to ensure compliance with the Visa Rules and specifically, the obligation to submit only legal Transactions into Interchange and only engage in legal Transactions.

- Ensure that the BPP:

  – Obtains active consent from the Obligee[2] to pay the biller on the Obligee's behalf and discloses the payment method used to pay the biller

  – Uses a Card product corresponding to the type of Obligee (i.e., a Consumer Debit Card product if the Obligee is an individual or a Commercial Card product if the Obligee is a business[3]), as listed in *Table 4-15, Bill Payment Providers Corresponding Card Products*

  – Allocates or uses a unique Account Range(s) or dedicated BIN(s) for each BPP aligned to the appropriate Card product and communicates to Visa the BPP name assigned to the relevant Account Range(s) or dedicated BIN(s)

  – Ensures appropriate disclosures relative to payment obligations, confirmation, and reimbursement responsibilities

  – Processes only Transactions where the Obligee's financial institution, the BPP and the biller are located in the same country

Table 4-15: Bill Payment Providers Corresponding Card Products

Obligee	Funding Source	Card Product
Individual	Consumer DDA at a U.S. Covered Financial Institution	U.S. Covered Consumer Debit Card
Individual	Consumer DDA at a U.S. Non-Covered Financial Institution	U.S. Non-Covered Consumer Debit Card

Table 4-15: Bill Payment Providers Corresponding Card Products (continued)

Obligee	Funding Source	Card Product
Individual	Cash	U.S. Non-Covered Consumer Debit Card
Business	Line of Credit / Good Funds Model / DDA	Visa Commercial Card

[1] An entity that provides a payment solution to facilitate individual or business bill payments on behalf of the Obligee or their financial institution using a Card to pay a biller when the payment is initiated as a bank transfer or cash payment.

[2] The individual consumer or business that is the recipient of the goods or services rendered by the biller, or is otherwise the biller's direct customer with respect to such goods or services as reflected on the customer account and billing statement.

[3] A business is any entity doing business, whether organized as a corporation, partnership, sole proprietorship, limited liability company, partnership, non-profit, or otherwise.

ID# 0030706	Edition: Apr 2020 | Last Updated: New

4.1.22   Card Personalization – Europe Region

4.1.22.1   Card Personalization Requirements – Europe Region (Italy)

In the Europe Region (Italy): An Issuer must ensure that all Cards are personalized to support Cash-Back.

ID# 0030093	Edition: Apr 2020 | Last Updated: Apr 2019

4.2   Visa Electron

4.2.1   Visa Electron Issuer Requirements

4.2.1.1   Visa Electron Program Features

An Issuer must ensure that its Visa Electron Program offers all of the following:

- Use for International Transactions[1] and Domestic Transactions

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Use for Electronic Commerce Transactions and other Card-Absent Environment Transactions[2]

- For Card-Present Environment Transactions (including ATM and Manual Cash Disbursements), both:
  - Signature or PIN verification
  - 100% Online Authorization

[1] Except as specified in *Section 4.1.1.5, Issuance of Domestic Use-Only Cards – AP, Canada, CEMEA, LAC, and US Regions*

[2] This does not apply in the LAC Region (Argentina, Brazil, Chile, Colombia, Mexico, Trinidad).

ID# 0004530	Edition: Apr 2020 | Last Updated: Oct 2017

4.2.1.2   Cardholder Instructions for Visa Electron Card Use

A Visa Electron Issuer must inform its Cardholders that a Visa Electron Card may be used:

- At a Merchant Outlet displaying the Visa Brand Mark with the Electron Identifier
- At an ATM displaying the Visa Brand Mark or Visa Brand Mark with the Electron Identifier

ID# 0004531	Edition: Apr 2020 | Last Updated: Oct 2014

4.3   Visa Check Card

4.3.1   Visa Check Card – Issuer Requirements

4.3.1.1   Visa Check Card Account Restrictions – US Region

In the US Region: A Visa Check Card may be used to access a deposit, investment, or other consumer asset account, including a fiduciary account.

A Visa Check Card must not be used to obtain credit, as defined in *12 CFR Part 226 (Regulation Z)*, unless it involves only an incidental extension of credit under an agreement between the Cardholder and the Issuer, either:

- When the Cardholder's account is overdrawn
- To maintain a specified minimum balance in the Cardholder's account

Visa reserves the right to determine the application of the definition of the Visa Check Card.

ID# 0008332	Edition: Apr 2020 | Last Updated: Oct 2016

4.3.1.2   Visa Check Card Activation – US Region

In the US Region: An Issuer must both:

- Require activation of all Visa Check Cards initially issued to Cardholders who did not expressly request or apply for the Visa Check Card

- As part of the activation process, require Cardholders to validate their identity by reasonable means before being able to use the Card

ID# 0004158	Edition: Apr 2020	Last Updated: Oct 2014

4.3.1.3   Visa Check Card Point-of-Sale Balance Inquiry – US Region

In the US Region: A Visa Check Card Issuer must not provide account balance information in response to a Point-of Sale Balance Inquiry on any of its Visa Check Card products.

ID# 0004161	Edition: Apr 2020	Last Updated: Oct 2015

4.3.2   Secured Card – Issuer Requirements

4.3.2.1   Secured Card Security Deposit Requirement – US Region

In the US Region: An Issuer must hold any cash security deposit for issuance of a Card in a federally insured account in the name of the Cardholder.

The Issuer must not assign an interest in a security deposit to any third party.

ID# 0008334	Edition: Apr 2020	Last Updated: Apr 2020

4.3.2.2   Secured Visa Card Solicitations – US Region

In the US Region: A Member or its Agent that solicits a secured Card account must do all of the following:

- Specify in its solicitation material that to obtain the Card, the potential Cardholder must open a deposit account that will serve as collateral for the Card account

- Indicate the portion of the deposit that will be allocated as the line of credit accessed by the Card

- Ensure that any secured Card application processing fees accepted from the Cardholder are made payable to the Issuer, not the Agent

ID# 0001217	Edition: Apr 2020	Last Updated: Apr 2020

Visa Product and Service Rules

4.4	Visa Gold

4.4.2 Visa Gold – Issuer Requirements

4.4.2.1 Visa Gold/Premier Card Issuance

A Visa Gold Card or Visa Premier Card Issuer:

- Must comply with the global support services requirements, either independently or through Visa

- May offer its Visa Gold Cards or Visa Premier Cards as any type of payment device with an option to access any of the following:
  - Line of credit
  - Depository account
  - Other Cardholder assets available through the Issuer

- In the Europe Region (France): A Visa Premier Card Issuer must:
  - Provide a welcome pack, approved by Visa, for newly subscribed Cardholders, including the services associated and, at least twice a year, information on Merchant offers
  - Provide travel insurance and medical assistance for all trips, in accordance with the corresponding notice information

ID# 0004220	Edition: Apr 2020 | Last Updated: Oct 2017

4.4.2.2 Visa Gold and Platinum Cards Issued on a Visa Platinum BIN – CEMEA Region

In the CEMEA Region: A Visa Gold Card issued on a Visa Platinum BIN must comply with the Visa Gold Card design requirements.

ID# 0008339	Edition: Apr 2020 | Last Updated: Oct 2014

4.4.2.3 Visa Gold/Premier Issuer Certification – Europe Region

In the Europe Region: A Visa Gold/Premier Issuer must provide to Visa, at least 30 calendar days before issuance, an application for written certification from Visa certifying that its programs, systems, procedures, and services comply with the Visa Rules.

ID# 0029621	Edition: Apr 2020 | Last Updated: Oct 2016

4.4.3   Visa Gold – Features and Benefits

4.4.3.1   Visa Gold Card Product Requirements – AP Region (Japan)

In the AP Region (Japan): A Visa Gold Card Issuer must do all of the following:

- Provide a Minimum Spending Limit of JPY 500,000 to its Visa Gold Cardholders
- Provide travel accident insurance coverage and/or Cardholder rewards and benefits as specified in *Table 4-16, Visa Gold Product Minimum Level of Cardholder Rewards and Benefits – AP Region (Japan).*
- Submit to Visa in writing an official quote from an insurance company for both the travel accident insurance and any proposed new features at least 30 calendar days before its implementation
- Certify its compliance with all of the Visa Gold product requirements 90 calendar days before program launch

Table 4-16: Visa Gold Product Minimum Level of Cardholder Rewards and Benefits – AP Region (Japan)

	Travel accident insurance	Total benefit value from the four categories of insurance, retail, travel, and lifestyle, per year	Rewards
Credit	USD 500,000	USD 70	50 basis points
	N/A	USD 150	50 basis points
	USD 500,000	N/A	100 basis points
	N/A	USD 50	100 basis points
Debit	USD 500,000	N/A	50 basis points
	N/A	USD 20	50 basis points

ID# 0029987   **Edition: Apr 2020 | Last Updated: Oct 2017**

4.4.3.2   Visa Gold Card Auto Rental Collision Damage Waiver – Canada Region

In the Canada Region: A consumer Visa Gold Card Issuer may offer collision/loss damage insurance either:

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

- Through the Visa Auto Rental Collision Damage Waiver program

- Independently

If the Issuer offers the Visa Auto Rental Collision Damage Waiver program, the Cardholder may obtain information about the program through Visa Global Customer Care Services, unless Visa has approved alternate arrangements.

ID# 0008236	Edition: Apr 2020 | Last Updated: Apr 2016

4.5   Visa Platinum

4.5.1   Visa Platinum – Card Requirements

4.5.1.2   Visa Platinum Debit Card Product Name Requirements – AP Region (Australia)

In the AP Region (Australia): A Visa Platinum Debit Card Issuer must use either the product name "Platinum" or an alternative name that complies with all of the following:

- Reflects the status of a premium debit product

- Is a unique name to identify the product type

- Is easily recognizable by a Merchant

- Is clearly displayed on the front of the Card

- Is not used for any other Visa product type

- Is only shared with other payment network-branded products that target an equivalent customer segment

ID# 0029222	Edition: Apr 2020 | Last Updated: Apr 2020

4.5.2   Visa Platinum – Customer Service Requirements

4.5.2.1   Visa Platinum Card Customer Service Telephone Number – Europe Region

In the Europe Region: A Visa Platinum Card Issuer must provide to its Visa Platinum Cardholders a customer service telephone number available 24 hours a day, 7 days a week.

ID# 0029622	Edition: Apr 2020 | Last Updated: Oct 2016

4.5.3   Visa Platinum – Issuer Requirements

4.5.3.2   Visa Platinum Card Issuance Requirements – Canada Region

In the Canada Region: A Visa Platinum Card Issuer must comply with all requirements related to Visa Gold Cards.

ID# 0004413	Edition: Apr 2020 | Last Updated: Oct 2014

4.5.3.4   Visa Platinum Card Issuance Requirements – Europe Region (France)

In the Europe Region (France): A Visa Platinum Card Issuer must:

- Display the Visa Platinum URL (*visaplatinum.fr*) in all communications to Cardholders
- Implement a website enabling Cardholders to access all documents relating to Visa Platinum

ID# 0030078	Edition: Apr 2020 | Last Updated: Oct 2017

4.5.4   Visa Platinum – Features and Benefits

4.5.4.4   Visa Platinum Card Core Services – Europe Region

In the Europe Region: A Visa Platinum Card Issuer must do all of the following:

- Provide both of the following services, through contract with a service provider, to its Cardholders travelling outside the country of Card issuance:
  - Medical referral service. The service provider must do all of the following:
    - Supply the Cardholder with details of the nearest hospital or doctor
    - Appoint a qualified medical practitioner to establish the condition of the Cardholder during treatment and relay that information to the Cardholder and the Cardholder's family members
    - Offer telephone translation services between the Cardholder and the medical attendant
    - Offer to assist in arranging payment of emergency medical bills. The Cardholder is fully liable for payment of emergency medical bills.

– Legal referral service. The service provider must do all of the following:

  ▪ Supply the Cardholder with details of local attorneys, embassies, or consulates

  ▪ Offer to communicate details throughout the emergency to the Cardholder's family or associates

  ▪ Offer to assist in arranging payment of bail or emergency legal fees. The Cardholder is fully liable for payment of bail or emergency legal fees.

● Ensure that the services are available 24 hours a day, 7 days a week

● Notify its Cardholders of the availability of the emergency travel assistance services and provide them with the telephone number through which they may obtain these services.

ID# 0029616	Edition: Apr 2020 | Last Updated: Oct 2016

4.5.4.6   Visa Platinum Card Travel Rewards Program – LAC Region

In the LAC Region: An Issuer of a Visa Platinum Card issued as a Credit Card must provide a rewards program that offers Cardholders, through purchases with Visa Platinum Cards, the ability to accumulate points that can be redeemed for, at a minimum, airline travel.

The rewards program may be sponsored by Visa (Visa Rewards), an Issuer, or through an Airline Affinity/Co-Brand program.

Cardholders must not be assessed an additional fee for membership in the rewards program.

Visa Platinum Cards that are issued as Debit Cards are exempt from any obligation to offer any rewards programs.

ID# 0008813	Edition: Apr 2020 | Last Updated: Apr 2020

4.5.5   Visa Platinum Prepaid – Issuer Requirements

4.5.5.3   Visa Platinum Prepaid Card Program Issuance Requirements – Canada Region

In the Canada Region: A Visa Platinum Prepaid Card Issuer must do all of the following:

● Comply with the requirements for Prepaid Cards and *Section 4.11.1.1, Prepaid Card Issuance Requirements*

- Ensure all Visa Platinum Prepaid Cards are:
  - Issued as EMV Chip Cards with the Visa Contactless Application
  - Issued for domestic and international use
  - Issued as Reloadable Cards and allow a minimum cumulative load of CAD 2,000
- Enable the Cardholder to do all of the following:
  - Have access to online account management (account balance, Transaction history)
  - Offer a mobile application that at a minimum allows the Cardholder to check balances and transaction history
  - Establish alerts via email, text message, or mobile application
- Provide an ongoing and relevant benefits or a rewards program

ID# 0029277	Edition: Apr 2020 | Last Updated: Apr 2020

4.6   Visa Rewards

4.6.3   Visa Rewards – Features and Benefits

4.6.3.2   Visa Rewards Product Benefits Requirements – AP Region (Australia)

In the AP Region (Australia): A Visa Rewards Product Issuer must provide its Visa Rewards Cardholders all of the following benefits:

Table 4-17: Visa Rewards Product Benefits – AP Region (Australia)

Benefit	Description
Cardholder Insurance[1]	Provide one or more insurance options to Visa Rewards Product Cardholders. The total unit cost per premium must match or exceed the current unit of cost providing USD 500,000 (or local currency equivalent) of travel accident insurance except where prohibited by applicable laws or regulations. The Issuer must submit to Visa in writing an official quote from an insurance company for both the travel accident insurance and the proposed new features at least 30 calendar days before its implementation.
Concierge Services[1]	Offer concierge services and must make these services available through a customer service attendant by telephone 24 hours a day, 7 days a week
Rewards Program	If it sets a cap on spend that earns rewards currency, not set such spend cap at less than X per month or X per year.

Table 4-17: Visa Rewards Product Benefits – AP Region (Australia) (continued)

Benefit	Description
	Communicate both of the following to its Visa Rewards Cardholders: • Visa benefits of the Visa Rewards Card at least twice per year • New benefits or changes to existing benefits at least 2 months before the effective date
Merchant Benefit[2]	An Issuer that opts to not offer a Minimum Spending Limit to its Cardholders must instead offer a Merchant-specific benefit (for example: free shipping, free expedited delivery, free goods and services) of AUD 100 per year.

[1] An Issuer may instead offer an alternative Cardholder benefit, as specified in *Section X.*

[2] This does not apply to an Issuer that offers its Cardholder an annual Minimum Spending Limit, as specified in *Section X.*

ID# 0029304   **Edition: Apr 2020 | Last Updated: Oct 2019**

4.6.4   Visa Traditional Rewards – Issuer Requirements

4.6.4.1   Visa Traditional Rewards Product Requirements – US Region

In the US Region: A Visa Traditional Rewards Card Issuer must comply with Visa Traditional product requirements, including, but not limited to, core service requirements.

ID# 0003883   **Edition: Apr 2020 | Last Updated: Oct 2014**

4.6.4.3   Issuer Rewards Program Registration – US Region

In the US Region: An Issuer must:

• Register its Visa Traditional Rewards program with Visa

ID# 0008806   **Edition: Apr 2020 | Last Updated: Apr 2015**

4.6.4.5   Visa Traditional Rewards Program Penalties for Non-Compliance – US Region

In the US Region: A Visa Traditional Rewards Card Issuer must meet the Visa Traditional Rewards Card product requirements to qualify for and receive the Visa Traditional Rewards Interchange

---

Reimbursement Fee (IRF), or it may be subject to non-compliance assessments.

ID# 0003899	Edition: Apr 2020 | Last Updated: Oct 2014

4.6.5   Visa Traditional Rewards – Features and Benefits

4.6.5.1   Visa Traditional Rewards Program Participation – US Region

In the US Region: A Visa Traditional Rewards Card Issuer must do all of the following:

- Offer a rewards program to its Visa Traditional Cardholders
- Notify Cardholders, at least quarterly, of their Rewards Currency via a stand-alone communication piece

ID# 0026236	Edition: Apr 2020 | Last Updated: Oct 2014

4.6.5.2   Visa Traditional Rewards Terms and Conditions – US Region

In the US Region: A Visa Traditional Rewards Card Issuer must comply with all of the following:

- Provide complete and accurate disclosure of all Visa Traditional Rewards Card terms and conditions, including, but not limited to, Rewards Currency, Rewards Currency accrual, expiration and maximum cap, point redemption, costs, fees (if any), an explanation of Qualifying Purchases, and all other material terms and conditions upon Cardholder enrollment in the program, and as required by applicable laws and regulations
- Communicate in writing the value of the Rewards Currency to its Cardholders, annually or as required by applicable laws or regulations, including, at minimum, all of the following information:
  - Amount earned
  - Amount redeemed
  - Balance remaining
- Notify the Cardholder of any material changes to the program terms and conditions before the revision effective date
- Ensure the accuracy of any information that it or its Agent provides to its Cardholders

ID# 0003897	Edition: Apr 2020 | Last Updated: Oct 2014

4.7   Visa Signature

4.7.1   Visa Signature and Visa Signature Preferred – Card Requirements

4.7.1.1   Visa Signature Card Requirements

A Visa Signature Card Issuer must include features and services equivalent to the Visa Infinite Card and all of the following:

- No pre-set spending limit[1]
- Access to web services specific to Visa Signature Cardholders
- A Card design specific to a Visa Signature Card

[1] In the US Region: This only applies to Visa Signature Cards issued as Visa Charge Cards.

ID# 0008228	Edition: Apr 2020 | Last Updated: Apr 2015

4.7.1.4   Visa Signature Card Point-of-Sale Spend Requirement – AP and CEMEA Regions

In the AP Region, CEMEA Region: A Visa Signature Card must meet the country-specific spend threshold established by Visa, failing which Visa may automatically modify the Interchange Reimbursement Fee (IRF) designation for the Card account using the spend qualification assessment. The IRF designation will be determined based on whether the Card account meets or does not meet the Visa Signature Card spend threshold.

Spend qualification assessment methodology may be defined by Visa within the specific country.

ID# 0027304	Edition: Apr 2020 | Last Updated: Oct 2014

4.7.2   Visa Signature and Visa Signature Preferred – Customer Service Requirements

4.7.2.1   Visa Signature Card and Visa Signature Preferred Card Customer Service Requirements – US Region

In the US Region: A Visa Signature Card and Visa Signature Preferred Card Issuer must do all of the following:

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

- Provide to its Cardholders a customer service toll-free telephone number available 24 hours a day, 7 days a week

- Ensure that the number is:

  - Serviced either by a customer service agent or a voice response unit

Issuers must also ensure access to account information 24 hours a day, 7 days a week through any or all of the following:

- Customer service agent

- A voice response unit

- Online access

ID# 0003906	Edition: Apr 2020 | Last Updated: Apr 2020

4.7.2.2   Visa Signature and Visa Signature Preferred Card Website – US Region

In the US Region: A Visa Signature and Visa Signature Preferred Issuer must provide its Cardholders access to a website that offers special information and services specific to its Visa Signature and Visa Signature Preferred Cardholders.

ID# 0003923	Edition: Apr 2020 | Last Updated: Oct 2014

4.7.3   Visa Signature and Visa Signature Preferred – Issuer Requirements

4.7.3.9   Visa Signature and Visa Signature Preferred Cardholder Notification – US Region

In the US Region: A Visa Signature or Visa Signature Preferred Issuer must provide notification to the Cardholder both:

- Before ongoing Transactions can be declined

- When an account needs to be suspended or closed for any reason

ID# 0003218	Edition: Apr 2020 | Last Updated: Oct 2014

4.7.3.10   Visa Signature Card Enhanced Billing Support – US Region

In the US Region: A Visa Signature Issuer must provide enhanced billing support resolution services to X.

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

ID# 0003907   Edition: Apr 2020 | Last Updated: Oct 2014

4.7.4   Visa Signature and Visa Signature Preferred – Features and Benefits

4.7.4.6   Visa Signature Card Travel Rewards Program – LAC Region

In the LAC Region: A Visa Signature Card Issuer must provide a rewards program that offers Cardholders, through purchases with Visa Signature, the ability to accumulate points that can be redeemed for Airline travel. The rewards program may be sponsored by Visa (Visa Rewards), an Issuer, or an Airline Affinity/Co-Brand program. Cardholders must not be assessed an additional fee for membership in the rewards program.

ID# 0004500   Edition: Apr 2020 | Last Updated: Oct 2015

4.7.4.7   Visa Signature and Visa Signature Preferred Spending Limits and Payment Options – US Region

In the US Region: A Visa Signature Issuer may allow a Visa Signature Cardholder the option to either:

- Pay in full each statement cycle. The Minimum Spending Limit for a Visa Signature Card issued as a Visa Charge Card must not be less than USD 2,000 per month.
- Revolve. This option does not apply to Visa Charge Cards.
  - For Visa Signature Cards, if positioned as a revolving product, the Issuer must permit a minimum revolving balance of at least USD 5,000 during each statement cycle.
  - For Visa Signature Preferred Cards, if the Visa Signature Preferred Cardholder is allowed the option to revolve, the Issuer must permit a minimum revolving balance of at least USD 5,000 during each statement cycle.

ID# 0008237   Edition: Apr 2020 | Last Updated: Apr 2018

4.7.4.8   Visa Signature and Visa Signature Preferred Rewards Program Participation – US Region

In the US Region: A Visa Signature or Visa Signature Preferred Issuer must both:

- Offer a rewards program to its Visa Signature or Visa Signature Preferred Cardholders
- Notify Cardholders, at least quarterly, via billing statement or stand-alone statement, of reward points earned during the relevant period

---

ID# 0003915	Edition: Apr 2020 | Last Updated: Oct 2014

4.8   Visa Infinite

4.8.1   Visa Infinite/Visa Infinite Privilege – Card Requirements

4.8.1.1   Visa Infinite Card Spending Limits

In the AP Region, CEMEA Region, Europe Region, LAC Region, US Region: A Visa Infinite Card Issuer[1,2] must offer such Cardholders either:

- A no pre-set limit, excluding Emergency Card Replacements
- A Minimum Spending Limit of X during each statement cycle in which a Cardholder has satisfied previous obligations to the Issuer.

[1] In the AP Region (Mainland China, India): This requirement does not apply to Issuers of Visa Infinite Cards issued as Debit Cards.

[2] In the AP Region (Singapore): This requirement does not apply to Issuers of Visa Infinite Cards issued as Debit Cards.

ID# 0004539	Edition: Apr 2020 | Last Updated: Apr 2020

4.8.1.2   Visa Infinite Card Features and Branding Requirements

A Visa Infinite Card Issuer must do all of the following:

- Offer features that differentiate the Visa Infinite Card from any other Card it issues
- Offer highest purchasing power available within the applicable Visa Region and the Issuer's Card portfolio, except when the Member-developed Card product:
  - Is not branded with a Card product name
  - Does not use the Sample Card Design or reserved color of a Card product
- In the US Region: Use the product name "Visa Infinite" on all Visa Infinite Cards and include it in all solicitations, advertising, promotions, and all its Cardholder communications

ID# 0004532	Edition: Apr 2020 | Last Updated: Apr 2020

4.8.1.4   Visa Infinite Business Minimum Spend Requirement – Europe Region

Effective 18 July 2020 In the Europe Region: A Visa Infinite Business program must meet the average minimum annual spend requirement at the portfolio level per account, ensuring that the

---

minimum spend levels exceed those of a Visa Platinum Business program. If the threshold is not met, the Issuer must implement a spend stimulation program.

ID# 0030689	Edition: Apr 2020	Last Updated: New

4.8.1.5   Visa Infinite Debit Card Issuance Requirements – AP Region (Mainland China, India, Singapore)

In the AP Region (Mainland China): An Issuer may provide a Visa Infinite Card issued as a Debit Card only to a Cardholder who has a minimum assets under management of X (or foreign currency equivalent) with the Issuer.

In the AP Region (India): An Issuer may provide a Visa Infinite Card issued as a Debit Card only to a Cardholder who has minimum assets under management of INR 3,000,000 with the Issuer.

In the AP Region (Singapore): An Issuer may provide a Visa Infinite Card issued as a Debit Card only to a Cardholder who has a minimum assets under management of SGD 500,000 with the Issuer.

ID# 0029457	Edition: Apr 2020	Last Updated: Apr 2020

4.8.2   Visa Infinite/Visa Infinite Privilege – Customer Service Requirements

4.8.2.2   Visa Infinite Card Emergency Services

If a Visa Infinite Issuer offers emergency services through the Visa Global Customer Assistance Services, it must do all of the following:

- Provide a toll-free or international collect-call telephone number 24 hours a day, 7 days a week
- Communicate the telephone number to the Cardholder annually
- In the US Region: In addition, both:
  - Activate and publish the domestic toll-free and international collect-call telephone number for emergency support
  - Provide the domestic toll-free number on the monthly billing statement.

ID# 0004544	Edition: Apr 2020	Last Updated: Oct 2019

4.8.2.3   Visa Infinite Cardholder Notification and Complaints

In the AP Region, Canada Region, CEMEA Region, Europe Region, US Region: A Visa Infinite Card Issuer must both:

- Provide advance notification to the Cardholder when an account needs to be suspended or closed for any reason

- Monitor customer complaints related to Transaction Authorizations

ID# 0004543	Edition: Apr 2020	Last Updated: Apr 2017

4.8.2.6   Visa Infinite Business Card Customer Service Requirements – Europe Region

Effective 18 July 2020 In the Europe Region: A Visa Infinite Business Card Issuer must do all of the following:

- Provide to its Cardholders access to a customer service agent 24 hours a day, 7 days a week

- Enable Cardholder access to trained dispute resolution service representatives through the Issuer's toll-free customer service number

- Ensure that the call center support meets or exceeds all of the following standards:

  – 90% of calls answered within 20 seconds

  – Wait time not to exceed 90 seconds

  – Conference calls transferred to a live agent

- Provide a domestic toll-free and international collect-call telephone number for account inquiries and emergency support. The domestic toll-free number must also appear on the monthly billing statement.

- At least annually, communicate the domestic and international telephone numbers independently or via email or billing statement

ID# 0030701	Edition: Apr 2020	Last Updated: New

4.8.3   Visa Infinite/Visa Infinite Privilege – Issuer Requirements

4.8.3.1   Visa Infinite Card/Visa Infinite Privilege Card Permitted Account Types

At the option of Visa, a Visa Infinite Card Issuer may support the following account types:

- In the AP Region, CEMEA Region, Europe Region: A credit, charge, or debit account

- In the Canada Region: For Visa Infinite Cards, a credit, charge, or debit account

- In the Canada Region: For Visa Infinite Privilege Cards, a credit or charge account

- In the LAC Region: A credit, charge, or debit account, or Prepaid Account

- In the US Region: A credit or charge account

ID# 0004537 | Edition: Apr 2020 | Last Updated: Apr 2020

4.8.3.6   Visa Infinite Privilege Program Compliance with Visa Infinite Rules – Canada Region

In the Canada Region: A Visa Infinite Privilege Card Issuer must comply with all requirements related to the Visa Infinite Card program.

ID# 0027692 | Edition: Apr 2020 | Last Updated: Oct 2014

4.8.3.8   Declined Visa Infinite Privilege Card Transactions – Canada Region

In the Canada Region: For Visa Infinite Privilege Cards issued with a no pre-set spending limit, an Issuer must provide notification to the Cardholder before ongoing Transactions may be declined.

ID# 0027701 | Edition: Apr 2020 | Last Updated: Oct 2014

4.8.3.9   Visa Infinite Privilege Card Marketing – Canada Region

In the Canada Region: A Visa Infinite Privilege Card Issuer must promote the Visa Infinite Privilege features, benefits, and services to Cardholders

ID# 0027702 | Edition: Apr 2020 | Last Updated: Apr 2017

4.8.3.13   Visa Infinite Card Delinquent Account Notification – Europe Region

In the Europe Region: For Visa Infinite Cards with no pre-set spending limit, an Issuer must provide notification to the Cardholder before declining any Transactions.

ID# 0029626 | Edition: Apr 2020 | Last Updated: Oct 2016

4.8.3.16   Visa Infinite and Visa Infinite Business Requirement to Provide Cardholder Disclosure – US Region

In the US Region: A Visa Infinite Card and a Visa Infinite Business Card[1] Issuer must disclose all of the following to its Cardholders:

- Information related to Card benefits arranged by the Issuer with third parties

- That it may provide personal Cardholder data to Visa, its contractors, or to Third-Party Agents for the purpose of providing Emergency Card Replacement, Emergency Cash Disbursement, or other Card-related benefits and services
- That to the extent personal Cardholder data is provided or disclosed to obtain travel and lifestyle or insurance benefits, the benefit providers will handle such information in accordance with their privacy policies

The Issuer must obtain Cardholder consent to the release of this information as a condition of obtaining a Visa Infinite Card or a Visa Infinite Business Card[1].

[1] **Effective 19 October 2019**

ID# 0029251	Edition: Apr 2020 | Last Updated: Apr 2020

4.8.3.17   Visa Infinite Card Issuance Requirements – Europe Region (France)

In the Europe Region (France): A Visa Infinite Card Issuer must:

- Display the Visa Infinite URL (*visainfinite.fr*) in all communications to Cardholders
- Implement a website enabling Cardholders to access all documents relating to Visa Infinite

ID# 0030079	Edition: Apr 2020 | Last Updated: Oct 2017

4.8.4   Visa Infinite/Visa Infinite Privilege – Features and Benefits

4.8.4.1   Visa Infinite Card Minimum Benefits

In the AP Region, Canada Region, CEMEA Region, Europe Region, US Region: A Visa Infinite Card Issuer must provide enhanced benefits to its Cardholders for all the following benefit categories:[1]

- Priority assistance and convenience
- Exclusive privileges and rewards
- Safety and security

In the AP Region (India): This does not apply to an Issuer of Visa Infinite Cards that are Debit Cards.

[1] In the AP Region (Cambodia, Myanmar): An Issuer may instead offer an alternative Cardholder benefit.

ID# 0008311	Edition: Apr 2020 | Last Updated: Apr 2020

4.8.4.2   Visa Infinite Card Web Services

In the AP Region,[1] Canada Region, CEMEA Region, Europe Region, US Region: A Visa Infinite Card Issuer must, either independently or through Visa, offer its Cardholders access to a website that offers special information and services to high-end consumers.

The Visa Infinite website must comply with all of the following:

- Be limited to Cardholders of Visa Infinite Cards
- Provide a description of Visa Infinite Card services, benefits, and features
- Provide a detailed listing of the Visa Infinite Exclusive Privileges Merchant partner offers
- Include all of the following minimum value-added content and services for travel and entertainment:
  – Travel-related content not readily available from other sources
  – Online concierge service, if concierge service is offered by the Visa Region or Member's Infinite product
  – Contact information for Cardholders to inquire about Visa Infinite services and to provide feedback
- In the US Region: In addition, both:
  – Enable Cardholder access to the Visa Infinite benefits portal hosted by Visa on behalf of the Issuer
  – Comply with the Visa content guidelines and approval requirements for any offers or content provided by or on behalf of the Issuer for use in connection with the Visa Infinite benefits portal

[1] In the AP Region (India): This requirement does not apply to Issuers of Visa Infinite Cards that are Debit Cards.

ID# 0008415   Edition: Apr 2020 | Last Updated: Apr 2020

4.8.4.13   Visa Infinite Privilege Card Website – Canada Region

In the Canada Region: A Visa Infinite Privilege Card Issuer must provide its Cardholders exclusive access to the Visa Infinite Privilege website that:

- Details information about Visa Infinite Privilege Card features, services, and benefits
- Enables Cardholders to link from the Issuer website to the Visa Infinite Privilege dedicated website

ID# 0027703   Edition: Apr 2020 | Last Updated: Oct 2014

4.8.4.15   Visa Infinite Card Core Features – Europe Region

In the Europe Region: A Visa Infinite Card Issuer must provide all of the following core services to its Cardholders:

- Both of the following safety and security features:
  - Medical referral, assistance, and emergency services
  - Legal referral, assistance, and Cash Disbursement services
- Both of the following priority assistance and convenience features:
  - Customer service representatives available 24 hours a day, 7 days a week
  - Concierge service
- Merchant partner program

ID# 0029624   Edition: Apr 2020 | Last Updated: Oct 2016

4.8.4.26   Visa Infinite Business Card Core Features – Europe Region

Effective 18 July 2020 In the Europe Region: In addition to the services specified in *Section 4.8.2.6, Visa Infinite Business Card Customer Service Requirements – Europe Region,* a Visa Infinite Business Card Issuer must provide to its Cardholders at least 4 services tailored to the product offering, where one of these services must be insurance. The services offered must have an equivalent market value of at least EUR 200 (or local currency equivalent).

ID# 0030690   Edition: Apr 2020 | Last Updated: New

4.8.4.27   Visa Infinite Business Card Operating Certificate Requirements – Europe Region

Effective 1 July 2020 In the Europe Region: A Visa Infinite Business Card Issuer must report its Visa Infinite Business Card activity separately through the Operating Certificate.

ID# 0030691   Edition: Apr 2020 | Last Updated: New

4.10   Campus Cards

4.10.1   Campus Card – Issuer Requirements

4.10.1.1   Campus Card Issuance – US Region

In the US Region: Participation in a Campus Card program is limited to principal Issuers and Sponsored Members.

A Campus Card Issuer must do all of the following:

- Limit issuance of a Visa Campus Card to:
  - A Debit Card or a Prepaid Card
  - "Active" student, staff, or faculty members at colleges and universities as defined by the Issuer in association with each school. "Active" status must be associated with the Cardholder's academic or employment status with the school.
- Ensure that any student identification number printed on the Campus Card does not contain any portion of the student's Social Security Number, the Payment Credential, or any other number that may present a privacy or security risk
- Limit issuance of a Campus Card to:
  - Identification
  - Building access
  - Library access
  - Other Visa-approved proprietary closed-loop applications
- Enable alternative network routing as required to comply with Regulation II

ID# 0027551   **Edition: Apr 2020 | Last Updated: Apr 2020**

4.10.1.2   Campus Card Extraneous Numbers or Devices – US Region

In the US Region: Any extraneous number or device embossed, printed, etched, encoded, or otherwise affixed to a Campus Card must not be used to facilitate any financial transactions, other than closed-loop proprietary college or university system transactions.

ID# 0027553   **Edition: Apr 2020 | Last Updated: Oct 2014**

4.11   Prepaid

4.11.1   Prepaid – Issuer Requirements

4.11.1.1   Prepaid Card Issuance Requirements

A Prepaid Card Issuer must:

- Obtain Visa approval prior to implementing a Prepaid Card program

- Adhere to anti-money laundering and anti-terrorist financing requirements

- Prohibit unauthorized reselling of its Prepaid Cards or Prepaid Accounts

- Not issue Prepaid Cards as any type of consumer credit program that extends a line of credit

- Ensure that the expiration date encoded on the Magnetic Stripe and Chip (when used) and embossed or printed on the Prepaid Card (if applicable) does not exceed 5 years from the date of issuance

- Provide a customer service telephone number to Cardholders

- Support Authorization Reversals

ID# 0003633   **Edition: Apr 2020 | Last Updated: Apr 2020**

4.11.1.3   Prepaid Card Funds and Reserves Requirements

A Prepaid Card Issuer must establish fund reserves to cover Prepaid Card Transactions and Settlement obligations. The Issuer must do all of the following:

- Ensure that prepaid funds are used only for valid Presentments

- Ensure that reserves are used only to cover direct program losses

- Monitor Agent reserves and account funding, including that of Mobile Network Operators (MNOs), and have access to Agent and MNO systems

- Periodically review and monitor Cardholder funds, including exception reporting

- In instances where the settlement or movement of funds between a Prepaid Card Issuer and its Agent is delayed, Issuers must ensure timely settlement of funds with their Agents to be compliant with Visa Issuer settlement requirements

A Prepaid Card Issuer must hold and control all Prepaid Card funds and Agent reserves in an account controlled by the Issuer. This requirement does not apply to:

- Members in countries where applicable laws or regulations require funds to be held in approved trust accounts

- In the US Region, Issuers of Visa Health Savings Account (HSA) programs, where funds must be held in an IRS-approved trust account

- Issuers of Visa Mobile Prepaid where funds are held with an Issuer-approved MNO's financial institution partner

- In the US Region, funds on deposit at an organization other than the Issuer's, as specified in *Section 4.1.1.11, Card Accessing Cardholder Funds on Deposit – US Region*

A Visa Mobile Prepaid Issuer must:

- Establish and hold reserves from the MNO to cover Card Transactions and Visa Settlement obligations

- Perform annual due diligence on the MNO's financial institution partner

ID# 0027830	Edition: Apr 2020	Last Updated: Apr 2020

4.11.1.4   Prepaid Account Balances

An Issuer must disclose its obligation for Prepaid Card balances to its Cardholder. The disclosure must comply with all of the following:

- Be either in writing or other appropriate means as approved by Visa

- Identify the Issuer responsible for Prepaid Account balances either on the front or back of the Card

- Not imply that Visa is liable for outstanding balances

ID# 0008353	Edition: Apr 2020	Last Updated: Apr 2020

4.11.1.8   Point-of-Sale Balance Inquiry and Point-of-Sale Balance Return Service – Issuer Participation Conditions

An Issuer that participates in the Point-of-Sale Balance Inquiry and/or a Point-of-Sale Balance Return Service must complete systems testing with Visa.

ID# 0025545	Edition: Apr 2020	Last Updated: Oct 2018

4.11.1.11   Prepaid Card Transaction Data Requirements – LAC Region (Brazil)

In the LAC Region (Brazil): An Issuer of a Prepaid Card must be able to receive the Merchant legal name and Merchant tax identification number in the Clearing Record for a Transaction completed with a Prepaid Card of government programs.

ID# 0029035	Edition: Apr 2020 | Last Updated: Apr 2020

4.11.1.14   Visa Consumer and Government Disbursement Reloadable Prepaid Cards – Issuer Requirements – Canada Region

In the Canada Region: An Issuer of a Visa Consumer Card or government disbursement Reloadable Prepaid Card[1] must do all of the following:

- Not charge the Cardholder a fee for domestic point-of-sale and domestic Card-Absent Environment Transactions

- Offer free access to financial education and tools to the Cardholder and clearly communicate available financial education and tools in Cardholder communications and where the Reloadable Prepaid Card is being promoted[2]

- Enable the Cardholder to:

  – Reload funds on the Card through one free method, including, but not limited to, bill payment, bank transfers, retail load hubs, direct deposit, Credit Card or Debit Card, cash, person-to-person funds transfer, mobile remote check deposit, or point-of-sale reload network

  – Check available balance through one free method, including, but not limited to internet, integrated voice response (IVR), or ATM

[1] This does not apply to travel Prepaid Cards issued in foreign currency and Visa Commercial Card Issuers.

[2] Financial education tools may be Issuer-proprietary (Issuer-branded, -owned, and -developed) or developed by third parties, as long as the Issuer provides the links to those resources.

ID# 0029459	Edition: Apr 2020 | Last Updated: Apr 2020

4.11.5   Prepaid – Distribution of Cards Outside the Country of Issuance

4.11.5.1   Limitation on Distribution of Prepaid Cards Outside the Country of Issuance

An Issuer authorized to distribute Prepaid Cards outside its country of Issuance must limit such distribution to Prepaid Cards that are funded solely by a multinational corporation or a government entity.

For Prepaid Cards distributed outside the country of issuance and funded by a multinational corporation, the Issuer must do all of the following:

- Be licensed to issue Cards in the country in which the multinational corporation has its global or regional headquarters[1]

- Obtain prior written approval from Visa for each Prepaid Card program enabled for distribution in a different country

- Not engage in any activity that amounts to active solicitation and issuance outside the countries in which it holds a Visa license

- Ensure compliance with local laws and regulations in each country of distribution

- With the exception of corporate disbursement cards issued as incentive cards to employees, ensure that at least 50% of the Prepaid Cards issued to the multinational corporation are distributed in countries in which the Issuer holds a Visa license

- For corporate incentive programs, ensure that the number of Prepaid Cards distributed in any single country does not exceed the number distributed in the country in which the Issuer holds a Visa license and the multinational corporation is headquartered

- For a Prepaid Card funded for the purpose of insurance-to-consumer programs, ensure that the insurance company is located within the country of the Issuer and Cards are provided only to policy holders who are living abroad. Centralized global Card distribution for global or multinational insurance companies is prohibited.

For Prepaid Cards distributed outside the country of issuance and funded by a government entity, the Issuer must ensure that both:

- No more than 25% of the total beneficiaries of the government disbursements under the specified government program reside outside the country of the Issuer

- The government entity is located within the same country as the Issuer

[1] This restriction does not apply to Airlines, Cruise Lines, and sea-based shipping companies.

ID# 0026802   Edition: Apr 2020 | Last Updated: Apr 2020

4.11.6   Prepaid – Authorization Services/Funds Access

4.11.6.1   Prepaid Card Selective Authorization

A Prepaid Card Issuer's systematic decline responses to Authorization Requests for specific Prepaid Cards must be based only on the following criteria:

- MCC

- Merchant name or terminal identification

- Location or Merchant Outlet

A Prepaid Card Issuer must obtain approval from Visa before implementing Selective Authorization programs or limiting acceptance, except when the Issuer suspects fraudulent or unusual activity.

ID# 0025537	Edition: Apr 2020	Last Updated: Apr 2020

4.11.6.2   Partial Authorization Service – Issuer Requirements

A Prepaid Card Issuer and its VisaNet Processor that offers Partial Authorization must support Partial Authorization Transactions and Authorization Reversals.

In the Canada Region and US Region: A Prepaid Card Issuer and its VisaNet Processor must support Partial Authorization Transactions.

In the CEMEA Region (Kenya, Russia, Serbia, Ukraine): An Issuer and its VisaNet Processor must support Partial Authorization service for domestic POS Transactions with Cash-Back.

ID# 0002494	Edition: Apr 2020	Last Updated: Apr 2020

4.11.7   Prepaid – Partners

4.11.7.2   Prepaid Partner – Load Partner Requirements

In addition to the requirements specified in *Section X*, a Prepaid Partner that provides Load Transaction services must do all of the following:

A Prepaid Partner that participates in Load and Activation services must obtain Issuer approval of an activation and load Authorization Request for Card activation for both Reloadable Prepaid Cards and Non-Reloadable Prepaid Cards.

ID# 0028182	Edition: Apr 2020	Last Updated: Apr 2020

4.11.10   Prepaid – Visa TravelMoney

4.11.10.1 Visa TravelMoney Participation

A Prepaid Card Issuer that participates in the Visa TravelMoney program must comply with all of the following:

- Participate in the Card Verification Service
- Issue pre-assigned or customer-selected PINs to all Visa TravelMoney Cards
- Accept PIN for Cardholder verification at an ATM
- Support ATM Cash Disbursements at both Visa/Plus ATM and Manual Cash Disbursements at Visa Member offices
- Not position Visa TravelMoney Cards as equivalent to Traveler's Cheques

ID# 0002503   Edition: Apr 2020 | Last Updated: Oct 2014

4.11.10.2   Visa TravelMoney Student Card Issuer Requirements – LAC Region

In the LAC Region: A Visa TravelMoney Student Card Issuer must both:

- Issue Cards as a Chip-enabled Prepaid Card
- Enable both Point-of-Transactions and ATM functionality on its Visa TravelMoney Student Cards

ID# 0029272   Edition: Apr 2020 | Last Updated: Apr 2019

4.11.10.3   Visa TravelMoney Student Card Core Benefits – LAC Region

In the LAC Region: A Visa TravelMoney Student Card Issuer must, at a minimum, provide to its Cardholders all of the following core product benefits, unless prohibited by applicable laws or regulations:

- Rental car insurance, including country of residence
- Travel and Emergency Assistance Services
- Visa Purchase Protection
- Visa Price Protection
- Visa Extended Warranty
- Visa Trip Delay
- Visa Luggage Delay

ID# 0029271   Edition: Apr 2020 | Last Updated: Oct 2017

4.11.10.4   Visa TravelMoney – Access to Funds – US Region

In the US Region: If an Issuer offers multiple Visa TravelMoney Cards to a Cardholder, the Issuer must both:

- Ensure full access to Visa TravelMoney funds for each Visa TravelMoney Card held by the Cardholder. If one or more Visa TravelMoney Cards are lost, the remaining Cards must still have access to funds.
- Replace one or more Cards up to the total number of Visa TravelMoney Cards originally purchased if one or more are lost, stolen, or damaged.

ID# 0008403	Edition: Apr 2020 | Last Updated: Oct 2015

4.11.10.5 Visa TravelMoney – ATM and POS Functionality

An Issuer that is licensed only for the issuance of Visa TravelMoney Cards must restrict the functionality on the Card to ATM use only.[1]

[1] This does not apply to Visa TravelMoney Student Cards.

ID# 0025548	Edition: Apr 2020 | Last Updated: Oct 2015

4.11.10.6 Visa TravelMoney Cardholder Notification

An Issuer of Visa TravelMoney Cards must inform its Cardholders that a Visa TravelMoney Card may be used at a Visa/Plus ATM location.

ID# 0002511	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.11   Prepaid – Visa Buxx

4.11.11.1 Visa Buxx Card Issuer Implementation Requirements – US Region

In the US Region: At least 30 days before issuing Cards, a Visa Buxx Issuer must submit to Visa written certification that its programs, systems, procedures, and services can support Visa Buxx Card requirements.

ID# 0004361	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.11.2 Visa Buxx Card Issuer Requirements – US Region

In the US Region: A Visa Buxx Issuer must designate a parent or an adult sponsor as the account owner of the Card with the option for the minor/underage person to be an authorized user:

A Visa Buxx Issuer must comply with all of the following:

- Not market a Visa Buxx Card to an underage person and decline the application if the intended authorized user is under the age of 13

- Offer the account owner the option to:

  – Establish defined spending and cash access limits by Transaction amount, type, and/or frequency

  – Receive text message, email or mobile application notifications when the limits are exceeded

  – Support on-demand, scheduled, or recurring minimum balance reloads in at least 3 ways, one of which must make funds available to the Cardholder within one hour of initiating the load

- Either itself, through Visa, or a third-party provider, offer:

  – Parental notification of payment activity and current balance information

  – The option to receive paper and/or electronic delivery of periodic Card statements

  – The ability to manage the account online

  – The ability to check available balance via internet, interactive voice response (IVR), or ATM

- Enable Cardholder access to funds through the Visa ATM network with a PIN if cash access is authorized on the account by the parent account holder.

ID# 0008378	Edition: Apr 2020 | Last Updated: Apr 2019

4.11.13   Prepaid – Employee Benefits/Healthcare

4.11.13.1 Visa Employee Benefit Card Issuer Requirements – US Region

In the US Region: A Prepaid Card Issuer must comply with both of the following:

- Not permit cash access for its Employee Benefits Cards

- Support Retrieval Request reason code 27 (Healthcare Auto-Sub Data Retrieval Request), for the purpose of obtaining detailed Transaction Receipt data from Acquirers, via fax, for Visa Flexible Spending Accounts (FSA) or Visa Health Reimbursement Arrangement (HRA)

ID# 0008386	Edition: Apr 2020 | Last Updated: Apr 2020

4.11.14   Prepaid – Visa Mobile

4.11.14.1 Visa Mobile Prepaid General Requirements – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Member participating in Visa Mobile Prepaid must do all of the following:

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

- Receive Original Credit Transactions, where available

- Ensure that all Visa Mobile Prepaid accounts are linked to a valid mobile telephone number

- Provide Visa with mobile phone number (Mobile Subscriber Integrated Services Digital Network-Number – MSISDN) to Account Number mapping data for each active Visa Mobile Prepaid account

ID# 0027159	Edition: Apr 2020 | Last Updated: Oct 2019

4.11.14.2 Visa Mobile Prepaid Issuer Requirements – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Visa Mobile Prepaid Issuer must do all of the following:

- Use a unique Visa Mobile Prepaid product sub-type and a Prepaid Card BIN assigned to a Visa Consumer Card, Visa Business Card, or Visa Commercial Card

- Ensure that a physical companion Card issued for a virtual Visa Mobile Prepaid account complies with the same branding requirements as any other Card

- Inform the Visa Mobile Prepaid user of any fees that may be charged

- Comply with the routing directory requirements

- Issue commercial Visa Mobile Prepaid Accounts to its Mobile Money Agents if participating in interoperable Mobile Money Agent services

- Support authentication for all Visa Mobile Prepaid Transactions

ID# 0027160	Edition: Apr 2020 | Last Updated: Apr 2020

4.11.14.3 Visa Mobile Prepaid Quarterly Reporting – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Member participating in the Visa Mobile Prepaid Program must report its Visa Transactions in its Operating Certificate.

ID# 0027161	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.14.4 Visa Mobile Prepaid Companion Card Requirements – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Visa Mobile Prepaid Issuer that makes a companion Card available to a Visa Mobile Prepaid account holder must both:

- Ensure that the Card does not have an expiration date of more than 5 years from the date of issuance

- Encode the Magnetic Stripe with an "X2X" Service Code

ID# 0027162	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.14.5 Visa Mobile Prepaid Processing Requirements – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: All Visa Mobile Prepaid Transactions completed on a BIN must be processed through VisaNet.

ID# 0027684	Edition: Apr 2020 | Last Updated: Oct 2019

4.11.14.6 Visa Mobile Money Operator Requirements – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Mobile Money Operator must do all of the following:

- Register as a Third Party Agent if it is not the licensed Issuer of Visa Mobile Prepaid

- Monitor its Mobile Money Agents for signs of fraud or other illegal activity

- Maintain an accurate list of its Mobile Money Agents, which must be provided to Visa upon request

- Ensure that its Mobile Money Agents do not add fees to what is already charged by the Mobile Money Operator for services provided to Visa Mobile Prepaid account holders at the Mobile Money Agent location

ID# 0027163	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.14.7 Visa Mobile Money Operator Authentication Requirements – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Mobile Money Operator must do all of the following:

- Complete a Mobile Money Consumer Authentication, before sending an Authorization Request

- Complete a Mobile Money Agent Authentication, before completing a Transaction or sending an Authorization Request. Only a Mobile Money Operator may complete the Mobile Money Agent Authentication.

- Require the Visa Mobile Prepaid account holder to complete Mobile Money Consumer Authentication for a Transaction only from the mobile telephone registered to the account holder
- Protect the Visa Mobile Prepaid account holder's account passcode in the same way that a PIN is protected during a Transaction

ID# 0027680	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.14.8 Mobile Money Agent Authentication – AP, CEMEA, and LAC Regions

In the AP Region, CEMEA Region, LAC Region: A Mobile Money Operator must both:

- Ensure that a Mobile Money Agent completes a Mobile Money Consumer Authentication for a Transaction only from the mobile telephone registered to the account holder's Visa Mobile Prepaid account
- Protect the Mobile Money Agent's account passcode in the same way a PIN is protected during a Transaction

ID# 0027681	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.15   Prepaid – Payroll/Salary

4.11.15.1 Visa Payroll Card – Cardholder Identification

A Visa Payroll Card Issuer must implement Card activation procedures that require Cardholders to validate their identity by some reasonable means before being able to use the Card.

ID# 0025571	Edition: Apr 2020 | Last Updated: Oct 2014

4.11.15.2 Visa Payroll Card – Access to Wages

A Visa Payroll Card Issuer must support Cardholder access to funds through both:

- Visa ATM Network with a PIN
- Manual Cash Disbursements at a Branch

In the US Region: A Visa Payroll Card Issuer must enable Visa Payroll Cardholders to withdraw the full balance in the Account, without cost, both:

- At least once per month
- If wages are paid more frequently than weekly, at least once per week

ID# 0027972	Edition: Apr 2020 | Last Updated: Apr 2019

4.11.15.3 Visa Payroll Card – Federally Insured Cardholder Funds – US Region

In the US Region: Visa Payroll Card funds must be federally insured for the benefit of Visa Payroll Cardholders.

ID# 0027973	Edition: Apr 2020 | Last Updated: Apr 2015

4.11.16   Prepaid – Visa Vale

4.11.16.1 Visa Vale Issuer Participation – LAC Region (Argentina, Brazil)

In the LAC Region (Argentina, Brazil): An Issuer that participates in the Visa Vale program must authorize and settle Visa Vale Transactions.

ID# 0027355	Edition: Apr 2020 | Last Updated: Oct 2014

4.12   Visa Commercial Products

4.12.1   Commercial Card Issuance Requirements

4.12.1.1 Commercial Card Issuance

An Issuer may only issue Visa Commercial Cards to provide a means of payment for business-related goods and services[1,2] and must not issue a Visa Commercial Card to an individual, except as follows:

- Employees of public- or private-sector organizations, including sole proprietors and self-employed individuals

- Employees or contractors of an organization as part of an employer-sponsored program

- At the discretion of Visa, members of an affinity group or association that requires a means to pay for business-related goods and services and is represented by a public- or private-sector company

[1] In the US Region: This requirement does not apply to Visa Business Check Cards used to pay Debt.

[2] In the Europe Region: An Issuer must ensure that the terms and conditions provided to a Visa Commercial Cardholder explicitly state that the Visa Commercial Card must be used only as a means of payment for business expenditures.

ID# 0003173	Edition: Apr 2020 | Last Updated: Apr 2020

4.12.1.2   Commercial Products Core Feature Requirements

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Visa Commercial Card Issuer must provide the core features specified as follows. A description of each core feature is provided below the table.

In the Europe Region: A Visa Commercial Card Issuer must comply with the .

Table 4-18: Visa Commercial Card Core Feature Requirements – AP Region, Canada Region, CEMEA Region, LAC Region, and US Region

Core Feature	Visa Business Card and Visa Business Electron Card[1]	Visa Corporate Card[1]	Visa Purchasing Card[1]	Visa Platinum Business Card and Visa Signature Business Card[2,3]	Visa Infinite Business – US Region (Effective 19 October 2019)
ATM Access	X	X[4]	X	X	X
Central or Individual Billing		X	X[5]		
Centralized Billing[6]		X	X		
Local Currency Billing[6,7]	X	X	X	X	X
Service Level Standards[6,7]	X	X[4]	X	X	X
Charge Card[8]		X[5]	X[5]		X
Limited Corporate Liability[8]		X	X		
Management Information Reporting[6,9]		X[4]	X		X
Flexible			X		

Table 4-18: Visa Commercial Card Core Feature Requirements – AP Region, Canada Region, CEMEA Region, LAC Region, and US Region (continued)

Core Feature	Visa Business Card and Visa Business Electron Card[1]	Visa Corporate Card[1]	Visa Purchasing Card[1]	Visa Platinum Business Card and Visa Signature Business Card[2,3]	Visa Infinite Business – US Region (Effective 19 October 2019)
Transaction Authorization [6,7,8]					
Individual Memo Statements[10]		X	X[5]		

1 In the LAC Region: Does not apply to Visa Business Electron Cards, Visa Corporate Electron Cards, and Visa Purchasing Electron Cards

2 In the CEMEA Region: Applies to Visa Platinum Business Cards and Visa Signature Business Cards

3 In the LAC Region: Applies to Visa Signature Business Cards and Visa Infinite Business Cards

4 In the LAC Region: Applies to Visa Corporate debit Cards

5 In the US Region: Core features required for Visa Purchasing Cards

6 In the LAC Region: Also applies to Visa Agro Cards

7 In the US Region: Does not apply to Visa Commercial Cards

8 Does not apply to Visa Corporate Prepaid Cards

9 In the AP Region (Malaysia): Also applies to Visa Signature Business Charge Cards and Visa Infinite Business Charge Cards

10 Applies to Visa Corporate Prepaid Cards

- ATM access: An Issuer must have the ability to offer a PIN to allow ATM Cash Disbursements, if requested. This ability is not required for Visa Purchasing Cards, unless requested by the customer. ATM access is not permitted for Vehicle-Specific Fleet Cards.

- Central or individual billing: An Issuer must offer the following billing options:

  - Individual Cardholder billing with individual payment

  - Individual Cardholder billing with centralized company payment

  - Centralized company billing and payment

- Local currency billing: An Issuer must have the ability to bill the subscribing company's Cardholders in the local currency of the country where the company and Cardholder physically reside

- Charge Card: An Issuer must have the ability to offer a non-revolving, pay-in-full option

- Limited corporate liability: An Issuer must be capable of providing insurance coverage to the subscribing company (where available) in the event of Visa Corporate or Visa Purchasing Card misuse by employees.

- In the Canada Region: An Issuer must provide insurance to protect businesses against unauthorized charges from misuse by employees with a minimum reimbursement of CAD 100,000 per Cardholder. Additional detailed information regarding insurance availability, options, and features is available from Visa upon request.

- Management information reporting: An Issuer must provide management information reports on Card usage to the subscribing company including:

  – Detailed Visa Corporate Card spending by vendor, employee, and company organization units

  – Detailed Visa Purchasing Card spending activity necessary to administer a Visa Purchasing Card program. Spending activity processing requirements may be defined by Visa

  – In the CEMEA Region: A detailed Visa Platinum Business Debit Card and Visa Signature Business Debit Card spending by employee

- Flexible Transaction Authorization: An Issuer must have the ability to restrict a purchase based upon a Transaction amount or Merchant Category Code specified by a client.

- Individual memo statements: An Issuer must have the ability to send a Transaction verification statement to each Cardholder.

ID# 0009018	Edition: Apr 2020 | Last Updated: Apr 2020

4.12.1.3   Commercial Products Mandatory Core Services

A Visa Commercial Card Issuer must provide to its Cardholders all of the core services specified as follows:

Table 4-19: Visa Commercial Card Mandatory Core Services

Mandatory Core Services	Visa Business Card[1]	Visa Corporate Card	Visa Purchasing Card
Medical referral, medical assistance, and emergency services[2,3,4]	X[5]	X	N/A
Legal referral, legal assistance, and cash disbursement services[2,3,4]	X[5]	X	N/A

Table 4-19: Visa Commercial Card Mandatory Core Services (continued)

Mandatory Core Services	Visa Business Card[1]	Visa Corporate Card	Visa Purchasing Card
Free 24-hour telephone number to obtain emergency services (Issuer must communicate the telephone number to the Cardholder at least once each year)[4]	X	X	X

[1] **Effective 19 October 2019** In the US Region: This requirement does not apply to Visa Infinite Business Cards.

[2] In the Europe Region: An exception to this requirement applies.

[3] This is an optional service for Visa Corporate Prepaid Cards.

[4] In the AP Region: This requirement does not apply for Visa Business Cards, Visa Corporate Prepaid Cards, or Visa Purchasing Cards.

[5] In the Canada Region: Medical referral, medical assistance, legal referral, and legal assistance are optional services for Visa Business Cards.

ID# 0003185   Edition: Apr 2020 | Last Updated: Apr 2020

4.12.1.4   Visa Commercial Card Issuer Certification – Europe Region

In the Europe Region: A Visa Commercial Card Issuer must provide to Visa, at least 30 calendar days before issuance, an application for written certification from Visa certifying that its programs, systems, procedures, and services comply with the Visa Rules.

ID# 0029628   Edition: Apr 2020 | Last Updated: Oct 2016

4.12.1.5   Visa Platinum Commercial Card Issuance – Europe Region

Effective through 17 April 2020 In the Europe Region: An Issuer may issue a Visa Platinum Commercial Card within an existing Visa Business Card or Visa Corporate Card program.

Effective 18 April 2020 In the Europe Region: An Issuer may issue a Visa Platinum Commercial Card within an existing Visa Corporate Card program.

ID# 0029635   Edition: Apr 2020 | Last Updated: Oct 2016

4.12.1.6   Requirements for Visa Commercial Cards that are Direct (Immediate) Debit Cards – Europe Region

In the Europe Region: An Issuer may issue a Visa Commercial Card that is a Direct (Immediate) Debit Card as either a Visa Business Card or Visa Business Electron Card.[1] The Card must be used to access a business current account or deposit/savings account, where purchases and Cash Disbursements arising from the use of that Card are posted to the account within the normal time for check clearing.

[1] In the Europe Region (Republic of Ireland, United Kingdom): An Issuer must not issue a Visa Business Electron Card.

ID# 0029636	Edition: Apr 2020 | Last Updated: Apr 2019

4.12.1.7   Visa Commercial Card Transaction Data Requirements – LAC Region (Brazil)

In the LAC Region (Brazil): An Issuer of Visa Commercial Cards must be able to receive the Merchant legal name and Merchant tax identification number in the Clearing Record for Transactions completed with Visa Commercial Cards of government programs.

ID# 0027383	Edition: Apr 2020 | Last Updated: Oct 2014

4.12.1.8   Visa Commercial Customer Service Telephone Number – US Region

In the US Region: An Issuer must provide customer assistance 24 hours a day, 7 days a week via a toll-free telephone number where its Visa Commercial Product Cardholders may obtain assistance while traveling.

ID# 0000417	Edition: Apr 2020 | Last Updated: Oct 2014

4.12.1.11 Visa Central Travel Account – Core Feature Requirements

All Visa Central Travel Account Issuers must do all of the following:

- Comply with the core feature requirements for the applicable product
- Offer electronic management information reports[1] at a company level detailing all spend relating to the company account on at least a monthly basis. The management information reports must include at a minimum all of the following:
  - Ticket number
  - Passenger name
  - Date of travel

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Provide travel accident insurance coverage when travel-related tickets are purchased using the Visa Central Travel Account. If standard policies do not include Visa Central Travel Accounts, Members must purchase coverage through Visa or another provider.

[1] In the Europe Region: If an Issuer uses Visa's service for the Visa Central Travel Account, it must comply with the terms of service and set up data feeds to Visa using the latest version of the Visa Commercial Format (or a format agreed by Visa).

ID# 0026398	Edition: Apr 2020 | Last Updated: Oct 2016

4.12.1.12   Visa Central Travel Account – Issuance Requirements

All Visa Central Travel Accounts must comply with all of the following:

- Issued using a Visa Corporate Card BIN or a Visa Purchasing Card BIN
- Issued to a Client Organization or a designated unit of the entity
- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Linked to a Virtual Account (when available) or to a physical Visa Card Account Number
- In the Europe Region: Issued as a Virtual Account
- In the Europe Region: Distinguished from other Visa Commercial Cards issued on the same BIN

ID# 0026396	Edition: Apr 2020 | Last Updated: Oct 2016

4.12.1.15   Centralized Card Issuance – Dual-Issuer Branded Visa Commercial Card Requirements

Only an Issuer that is a registered Visa Multinational Program participant may issue Dual-Issuer Branded Visa Commercial Cards.

The Lead Bank and the Partner Bank must be registered Visa Multinational Program participants and have contractual agreements with each other that clearly define the Dual-Issuer Branded Visa Commercial Card program.

The Issuer of a Dual-Issuer Branded Visa Commercial Card must be clearly identified on the back of the Card and in all Cardholder agreements.

A Dual-Issuer Branded Visa Commercial Card must be issued using a BIN that is licensed to the Partner Bank.

Before issuing Dual-Issuer Branded Visa Commercial Cards, the Lead Bank and the Partner Bank must provide contractual evidence of the partnership agreement to Visa for review and approval.

The Lead Bank must ensure that the Dual-Issuer Branded Visa Commercial Card program complies with all applicable laws or regulations in the country in which the Cards are issued and the country in which the Lead Bank is domiciled.

ID# 0026023	Edition: Apr 2020 | Last Updated: Oct 2014

4.12.1.16 Visa Commercial Card Product Types – US Region

In the US Region: An Issuer must refer to the Visa Commercial Card products as one of the following types of Cards for business expense use:

- Visa Business Card
- Visa Corporate Card or Visa Travel Card[1]
- GSA Visa Corporate Card
- Visa Purchasing Card

[1] Visa Travel Card is for use by public sector or non-profit entities that are not corporations.

ID# 0004214	Edition: Apr 2020 | Last Updated: Oct 2015

4.12.2   Commercial Data Management and Reporting

4.12.2.1   Visa Commercial Solutions Data and Reporting Tools Participation and Indemnification – AP, Canada, CEMEA, LAC and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Where available, an Issuer is authorized to grant Visa Commercial Solutions Data and Reporting Tools access and use to a Client Organization.

An Issuer participating in any Visa Commercial Solutions Data and Reporting Tools must do all of the following:

- Sign a participation agreement, where applicable, and comply with and ensure that their Client Organizations comply with applicable terms and documentation
- Ensure an agreement is in place with the Client Organization governing that entity's use of such Visa Commercial Solutions Data and Reporting Tools prior to granting a Client Organization access to and use of any tools
- Notify, or ensure that the Issuer's Client Organization notifies, individual Commercial Cardholders and obtain any required consents, in accordance with applicable laws or regulations, that certain

data concerning those Cardholders, including Enhanced Data, will be provided to the Issuer and the Issuer's Client Organization

- Comply, and ensure that its Client Organization complies, with any other applicable legal requirements that must be met to allow the provision of the Enhanced Data to the Issuer and the Issuer's Client Organization

The participating Issuer may not use any Enhanced Data for any marketing purposes.

An Issuer that is authorized to participate in Visa Commercial Solutions Data and Reporting Tools, and grants access and use to a Client Organization, Indemnifies Visa for and against Claims and Liabilities arising out of or in connection with a Client Organization's use of such tools and services.

ID# 0004236	Edition: Apr 2020 | Last Updated: Apr 2018

4.12.2.2   Visa Commercial Reporting and Data Services Limitations – US Region

In the US Region: All of the commercial reporting and data services provided by Visa are the property of Visa and are for the use of the Issuer and its Client Organization solely in support of its Visa Commercial Card products.

ID# 0001397	Edition: Apr 2020 | Last Updated: Apr 2020

4.12.2.3   Disclosure of Enhanced Data to Third Parties – US Region

In the US Region: Enhanced Transaction-Level Data and Confidential Enhanced Merchant-Level Data may be disclosed to third parties only either:

- In connection with the management and administration of Visa Commercial Card programs for the Client Organization, and necessary supporting functions, which may include, but are not limited to, accounting, tax management, policy compliance, and other business management functions, such as account setup and management reporting
- In aggregate, in such a way that Card-specific Enhanced Data cannot be related to a specific Merchant or Cardholder

Third party means only persons, real or corporate, other than the Issuer, Client Organization, or Cardholder, providing services that directly support an Issuer's Visa Commercial Card program.

These restrictions do not apply to Non-Confidential Enhanced Merchant-Level Data.

ID# 0004243	Edition: Apr 2020 | Last Updated: Oct 2015

4.12.2.4   Use and Disclosure of Card-Specific Enhanced Data – US Region

In the US Region: A Visa Commercial Card Issuer may use or disclose Card-specific Enhanced Data only in connection with the management and administration of a Visa Commercial Card program for the Client Organization, and necessary supporting functions.

ID# 0004242	Edition: Apr 2020	Last Updated: Oct 2015

4.12.2.5   Third Party Agreement for Enhanced Data Usage – US Region

In the US Region: If an Issuer discloses Card-specific Enhanced Transaction-Level Data or Confidential Enhanced Merchant-Level Data to a third party, it must have a written agreement with the third party that requires the third party to do all of the following:

- Treat the information as confidential
- Make no further disclosure of the information without permission
- Limit the third party's use of the data to uses permitted by the Issuer

Permission granted for further disclosure by a third party must impose the same restrictions on use and disclosure that apply to the Issuer's disclosure.

Each Issuer bears the sole responsibility for compliance with all applicable laws and regulations.

ID# 0004244	Edition: Apr 2020	Last Updated: Oct 2014

4.12.2.6   Visa Payables Automation Participation Requirements

An Issuer participating in the Visa Payables Automation service must ensure that it, and its participating clients or Client Organizations, comply with all of the following:

- Implement appropriate security and anti-fraud measures to ensure that all of the following:
  - The Payment Credentials are protected from misuse.
  - The payment instructions submitted to Visa are accurate.
  - Employees with administrative and user access rights adhere to security policies.
- Maintain administrative and user accounts and remove access rights for terminated employees immediately.
- Provide payables instructions to Visa that do not violate any existing supplier agreements.

ID# 0026534	Edition: Apr 2020	Last Updated: Apr 2020

4.12.2.7   Visa Purchasing Card Enhanced Data Requirements – Europe Region

In the Europe Region: In a country where Visa has obtained VAT accreditation agreements, a Visa Purchasing Card must be issued as an Enhanced Data product with VAT accreditation.[1]

An Issuer in these countries must both:

- Be able to receive and process the following data types:
  - Basic Transaction data
  - Enhanced Data for management information purposes that does not comply with VAT accreditation requirements
  - Enhanced Data that complies with VAT accreditation requirements
- Provide its clients with VAT evidence reporting

In a country where Visa has not obtained VAT accreditation agreements, an Issuer must configure its BINs and Account Ranges to receive and process Enhanced Data for management information purposes.

[1] This does not apply to Visa Drive Cards that are "extra" Cards, which must not be issued as Enhanced Data products with VAT accreditation.

ID# 0029629	Edition: Apr 2020 | Last Updated: Apr 2019

4.12.2.8   Visa IntelliLink Spend Management Participation – Europe Region

In the Europe Region: To participate in Visa IntelliLink Spend Management, an Issuer must do all of the following:

- Comply with the *Europe Region IntelliLink Spend Management Terms of Use*
- Comply with the *Europe Region IntelliLink Spend Management Services Participation Agreement*
- Set up data feeds to Visa IntelliLink Spend Management using the current version of the Visa Commercial Format or format as agreed to by Visa

ID# 0029632	Edition: Apr 2020 | Last Updated: Oct 2016

4.12.2.9   Data Field Processing Requirement – Europe Region

In the Europe Region: An Issuer must be able to process the additional data fields transmitted by an Acquirer in any processing records in accordance with the level of data capability of the BIN as specified by the Issuer.

ID# 0029634	Edition: Apr 2020 | Last Updated: Oct 2016

4.12.3   V Distribution Program

4.12.3.1   V Distribution Requirements

An Issuer participating in the V Distribution Program must comply with all of the following:

- Provide payment services to a V Distribution Program Cardholder purchasing goods and services from a V Distribution Program participating Merchant.
- Be certified to issue either:
  - Visa Purchasing Cards
  - Visa Business Cards
- Be registered with Visa
- Be capable of processing Authorization Requests, billing, and reporting

ID# 0003163	Edition: Apr 2020 | Last Updated: Oct 2015

4.12.4   Visa B2B Virtual Payments Program

4.12.4.1   Visa B2B Virtual Payments Product – Issuance Requirements

An Issuer participating in the Visa B2B Virtual Payments Program[1] must comply with all of the following:

- Obtain Visa approval prior to participating in the program
- Submit a *BIN License Agreement* or *Numeric License Agreement* to Visa to register the product
- Use the account only as a credit Card account within the commercial product type or, in addition, in the Europe Region, as a credit Card account or Deferred Debit Card account within the commercial product type
- Complete a separate Credit Card or Deferred Debit Card Schedule of the regional Operating Certificate to report product activity
- Offer the product as a Virtual Account and support the generation of a dynamic, virtual Account Number for Visa B2B Virtual Payments Program Transactions
- Offer the product to eligible business entities only for business-to-business payment for goods or services invoiced by a qualifying Merchant

- Ensure the Transaction is both:
  – For an amount below USD 750,000
  – Key-entered in a Card-Absent Environment
- If enrolled in the Authorization and Settlement Match Service, comply with the requirements specified by the service

¹ In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Not available in countries where Visa does not process Domestic Transactions or does not set the Interchange Reimbursement Fee (IRF). In the Europe Region: Not available in countries where Visa does not set the Interchange Reimbursement Fee.

ID# 0029994   Edition: Apr 2020 | Last Updated: Apr 2019

4.13   Visa Small Business Product-Specific Issuance

4.13.1   Visa Business – Card Requirements

4.13.1.1   Visa Business Card ATM Access Requirements – US Region

In the US Region: A Visa Business Card Issuer must provide ATM access.

ID# 0004247   Edition: Apr 2020 | Last Updated: Oct 2014

4.13.1.2   Visa Business Card Account Billing Options – US Region

In the US Region: An Issuer may offer its Visa Business Card Cardholders any of the following account billing options:

- Line of credit
- Depository account
- Other company assets available through the Issuer
- Charge Card (non-revolving, pay-in-full)

ID# 0004293   Edition: Apr 2020 | Last Updated: Oct 2014

4.13.1.3   Visa Business Check Card Account Limitations – US Region

In the US Region: An Issuer must not use a Visa Business Check Card to obtain credit, as defined in *12 CFR Part 226 (Regulation Z)*, unless it involves only an incidental extension of credit under an agreement between the Cardholder and the Issuer either:

- When the Cardholder's account is overdrawn

- To maintain a specified minimum balance in the Cardholder's account

For Interchange category purposes, a Visa Business Check Card used to obtain credit is not considered a Visa Business Check Card if both:

- Actual debiting of funds from the business asset account occurs periodically rather than daily

- These periods are at least X days apart

ID# 0008304	Edition: Apr 2020 | Last Updated: Oct 2014

4.13.1.4   Visa Business Check Card Account Access – US Region

In the US Region: A Visa Business Check Card may be used to access a deposit, investment, or other business asset account, including a fiduciary account.

ID# 0004252	Edition: Apr 2020 | Last Updated: Oct 2014

4.13.1.5   Unauthorized Visa Business Card Transaction Exclusions – US Region

In the US Region: An Issuer of Visa Business Cards may define an unauthorized Visa Transaction to exclude any Transaction allegedly conducted by:

- A business co-owner

- The Cardholder or person authorized by the Cardholder

- Any other person with an interest in or authority to transact business on the account

ID# 0000406	Edition: Apr 2020 | Last Updated: Oct 2014

4.13.3   Visa Business – Issuer Requirements

4.13.3.6   Visa Business Insurance Requirements – Europe Region (France)

In the Europe Region (France): A Visa Business Card Issuer must provide to Cardholders a welcome pack, approved by Visa, including the services associated and, at least once a year, information on Merchant offers.

ID# 0030080	Edition: Apr 2020 | Last Updated: Oct 2017

4.13.4   Visa Business – Features and Benefits

4.13.4.3   Visa Business Card Core Benefits – LAC Region

In the LAC Region: A Visa Platinum Business, Visa Signature Business, and Visa Infinite Business Card Issuer must, at a minimum, provide its Cardholders with all of the following core product benefits, unless prohibited by applicable laws or regulations:

Table 4-20: Visa Business Card Core Benefits – LAC Region

Core Benefit	Visa Platinum Business	Visa Signature Business	Visa Infinite Business
Travel Assistance Services	Worldwide	Worldwide	Worldwide
Price Protection	Up to USD 2,000 per year	Up to USD 2,000 per year	Up to USD 4,000 per year
Purchase Protection	Up to USD 25,000 per year	Up to USD 25,000 per year	Up to USD 25,000 per year
Extended Warranty	Up to USD 10,000 per year	Up to USD 10,000 per year	Up to USD 25,000 per year
Auto Rental Collision Damage Waiver	Worldwide	Worldwide	Worldwide
Travel Accident Insurance with accidental death benefit	Up to USD 500,000	Up to USD 1,000,000	Up to USD 1,500,000
International Emergency Medical Services	Up to USD 150,000	Up to USD 200,000	Up to USD 200,000
Baggage Delay	N/A	Up to USD 500	Up to USD 600
Baggage Loss	N/A	Up to USD 1,000	Up to USD 3,000
Missed Connection	N/A	N/A	Up to USD 300
Trip Delay	N/A	N/A	Up to USD 300
Trip Cancellation	N/A	N/A	Up to USD 3,000
Insured Journey	N/A	Up to USD 50,000	Up to USD 100,000

Table 4-20: Visa Business Card Core Benefits – LAC Region (continued)

Core Benefit	Visa Platinum Business	Visa Signature Business	Visa Infinite Business
Personal Concierge Service	Provided through Visa	Provided through Visa	Provided through Visa
Visa Luxury Hotel Collection	Provided through Visa	Provided through Visa	Provided through Visa
Priority Pass Membership	N/A	N/A	Complimentary membership for Core Priority Pass programs

ID# 0029971   Edition: Apr 2020 | Last Updated: Apr 2017

4.15   Visa Platinum Business

4.15.1   Visa Platinum Business – Card Requirements

4.15.1.3   Visa Platinum Business Cardholder Spending Limit – CEMEA Region

In the CEMEA Region: An Issuer that participates in Visa Platinum Business Card issuance must offer one of the following spending limit options to its Visa Platinum Business Cardholders:

- No pre-set spending limit except as permitted for:
  - Cash Disbursement Transaction
  - Transactions resulting from an Emergency Card Replacement
- A Minimum Spending Limit of USD 5,000 (or local currency equivalent), for Transactions during each statement cycle

The Issuer must allow a Visa Platinum Business Cardholder the option to either:

- Pay in full each statement cycle
- Revolve

ID# 0029162   Edition: Apr 2020 | Last Updated: Apr 2018

4.15.1.4   Visa Platinum Business Card – Card Design Requirements – CEMEA Region

In the CEMEA Region: The product name "Visa Platinum Business" must appear on the front of the Card.

A Visa Platinum Business Card Issuer must use the product name "Visa Platinum Business" in all solicitations, advertising, and promotions, Card account statements and other communications regarding Visa Platinum Business Cards.

ID# 0029163   Edition: Apr 2020 | Last Updated: Apr 2017

4.15.1.5   Visa Platinum Business Card Rewards Program – Europe Region

Effective 18 July 2020 In the Europe Region: A Visa Platinum Business Card Issuer must provide a rewards program to its Visa Platinum Business Cardholders that reasonably enables each Cardholder to redeem a minimum value equivalent to 10 basis points per EUR (or local currency equivalent) of qualifying spend, based on the combination of earn rates and redemption value.

ID# 0030696   Edition: Apr 2020 | Last Updated: New

4.15.1.6   Visa Platinum Business Card Rewards Program – LAC Region

In the LAC Region: An Issuer must provide a rewards program that offers Cardholders the ability to accumulate points for purchases made with a Visa Platinum Business Card.

Any travel rewards program offered to the Cardholder must be sponsored by Visa (Visa rewards), the Issuer, or an Airline Affinity/Co-Brand program. The Issuer must not assess any additional fees to the Cardholder for membership in the travel rewards program.

A Visa Platinum Business debit Card Issuer is not required to offer any travel rewards programs.

ID# 0027672   Edition: Apr 2020 | Last Updated: Oct 2015

4.15.2   Visa Platinum – Customer Service Requirements

4.15.2.1   Visa Platinum Business Card – Customer Service Requirements – CEMEA Region

In the CEMEA Region: A Visa Platinum Business Card Issuer must:

- Provide advance notification to the Cardholder when an account needs to be suspended or closed for any reason

- Monitor customer complaints related to Authorizations and make this information available to Visa

- Identify action plans to improve customer service

ID# 0029164   Edition: Apr 2020 | Last Updated: Apr 2017

4.15.3   Visa Platinum Business – Issuer Requirements

4.15.3.1   Visa Platinum Business Certification – LAC Region

In the LAC Region: Before issuing Visa Platinum Business Cards, an Issuer must receive written certification from Visa that it complies with all product requirements and standards.

ID# 0027663   Edition: Apr 2020 | Last Updated: Oct 2014

4.15.3.2   Visa Platinum Business Card Operating Certificate Requirements – Europe and LAC Regions

In the Europe Region,[1] LAC Region: A Visa Platinum Business Card Issuer must report its Visa Platinum Business Card Activity separately through the Operating Certificate.

[1] **Effective 1 July 2020**

ID# 0027662   Edition: Apr 2020 | Last Updated: Apr 2020

4.15.3.3   Visa Platinum Business Card Credit Limit – LAC Region

In the LAC Region: A Visa Platinum Business Credit Card Issuer must both:

- Preserve the premium status of the Visa Platinum Business Card by providing a higher credit limit for its Visa Platinum Business program than the average credit limit for its Visa Platinum and Visa Business programs

- Allow each Visa Platinum Business Card account to accumulate charges of at least 10% above the approved credit limit during each billing statement cycle in which the Cardholder has satisfied previous obligations to the Issuer

---

ID# 0027671   Edition: Apr 2020 | Last Updated: Oct 2014

4.15.3.5   Visa Platinum Business Card Payment Options – LAC Region

In the LAC Region: An Issuer must position its Visa Platinum Business Card only as a payment device that can access one of the following funding sources:

- A line of credit
- A depository account
- Other Cardholder assets available through the Issuer

4.15.3.6   Visa Platinum Business Card Minimum Spend Requirement – Europe Region

Effective 18 July 2020 In the Europe Region: A Visa Platinum Business program must meet the average minimum annual spend requirement at the portfolio level per account, ensuring that the minimum spend levels exceed those of a Visa Business program. If the threshold is not met, the Issuer must implement a spend stimulation program.

4.15.3.7   Visa Platinum Business Card Issuance Requirements – Europe Region (France)

In the Europe Region (France): A Visa Platinum Business Card Issuer must:

- Display the Visa Platinum Business URL (*visaplatinumbusiness.fr)* in all communications to Cardholders
- Implement a website enabling Cardholders to access all documents relating to Visa Platinum Business

4.15.4   Visa Platinum Business – Features and Benefits

4.15.4.2   Visa Platinum Business Cardholder Spend Reporting – CEMEA Region

In the CEMEA Region: A Visa Platinum Business Card Issuer must, either itself or through Visa Business Reporting, provide its Visa Platinum Business Cardholders a report, at least annually, that includes both:

- Total annual amount spent by Cardholder or company
- Summary of spending by Merchant category

ID# 0029171	Edition: Apr 2020 | Last Updated: Apr 2017

4.15.4.3   Visa Platinum Business Card Additional Core Services – CEMEA Region

In the CEMEA Region: A Visa Platinum Business Card Issuer, at its discretion, may provide:

- One or more travel accident insurance coverage options with a unit cost per premium that matches or exceeds the current unit cost of providing up to USD 500,000, (or local currency equivalent) of travel accident insurance. The Issuer must submit to Visa in writing, an official quote from an insurance company, for both the travel accident insurance and the proposed new features, at least 30 calendar days prior to its implementation.
- Emergency medical evacuation and repatriation services
- Emergency medical insurance when traveling, with medical expense benefit up to USD 50,000, or local currency equivalent

The Issuer must communicate all of the following Visa Platinum Business Card Privileges Program information to Cardholders:

- Visa Platinum Business Card Privileges Program benefits at least once a year
- New benefits or changes to existing benefits, or exclusive quarterly Merchant offers at least 2 months prior to the effective date of Visa Platinum Business Card Merchant Privileges

ID# 0029172	Edition: Apr 2020 | Last Updated: Apr 2017

4.15.4.4   Visa Platinum Business Card Core Features – Europe Region

Effective 18 July 2020 In the Europe Region: In addition to the services specified in *Section 4.15.4.5, Visa Platinum Business Card Customer Service Requirements – Europe Region,* a Visa Platinum Business Card Issuer must provide to its Cardholders at least 2 services tailored for the product offering, where one of these services must be insurance. The services offered must have an equivalent market value of at least EUR 100 (or local currency equivalent) on credit, and at least EUR 50 (or local currency equivalent) on debit.

ID# 0030694	Edition: Apr 2020 | Last Updated: New

4.15.4.5   Visa Platinum Business Card Customer Service Requirements – Europe Region

Effective 18 July 2020 In the Europe Region: A Visa Platinum Business Issuer must provide all of the following:

- Dedicated customer service 24 hours a day, 7 days a week

- Cardholder emergency services for Visa Platinum Business Cards

- An exclusive telephone line for its Visa Platinum Business Cardholders

ID# 0030695	Edition: Apr 2020 | Last Updated: New

4.16   Visa Signature Business

4.16.1   Visa Signature Business – Card Requirements

4.16.1.3   Visa Signature Business Cardholder Spending Limit – CEMEA Region

In the CEMEA Region: An Issuer that participates in Visa Signature Business Card issuance must offer one of the following spending limit options to its Visa Signature Business Cardholders:

- No pre-set spending limit except as permitted for:
  - Cash Disbursement Transaction
  - Transactions resulting from Emergency Card Replacement

- A Minimum Spending Limit of USD 10,000 (or local currency equivalent), for Transactions during each statement cycle

For Cards with no pre-set spending limit, a CEMEA Visa Signature Business Card Issuer must provide notification to the Cardholder before ongoing Transactions can be declined.

The Issuer must allow a Visa Signature Business Cardholder the option to either:

- Pay in full each statement cycle

- Revolve

ID# 0029175	Edition: Apr 2020 | Last Updated: Apr 2018

4.16.1.4   Visa Signature Business Card – Card Design Requirements – CEMEA Region

The product name "Visa Signature Business" must appear on the front of the Card.

In the CEMEA Region: A Visa Signature Business Card Issuer must use the product name "Visa Signature Business" in all solicitations, advertising, and promotions, Card account statements and other communications regarding Visa Signature Business Cards.

ID# 0029176	Edition: Apr 2020 | Last Updated: Apr 2017

4.16.1.5   Visa Signature Business Card Rewards Program – LAC Region

In the LAC Region: A Visa Signature Business Card Issuer must provide a rewards program that both:

- Offers Cardholders the ability to accumulate points for purchases made with a Visa Signature Business Card

- Is comparable to any existing Issuer's Visa Signature Card or Visa Infinite Card rewards program

Any travel rewards program offered to the Cardholder must be sponsored by Visa (Visa rewards), the Issuer, or an Airline Affinity/Co-Brand program. The Issuer must not assess any additional fees to the Cardholder for membership in the travel rewards program.

An Issuer of a Visa Signature Business Card issued as a Debit Card is not required to offer any travel rewards programs.

ID# 0029972   **Edition: Apr 2020 | Last Updated: Apr 2020**

4.16.1.6   Visa Signature Business Card Account Types and Credit Limit – LAC Region

In the LAC Region: With prior approval from Visa, a Visa Signature Business Card Issuer must offer such Card with credit or debit functionality.

An Issuer of a Visa Signature Business Card issued as a Credit Card must both:

- Preserve the premium status of the Visa Signature Business Card by providing a higher credit limit for its Visa Signature Business program than the average credit limit for its Visa Platinum, Visa Signature, and Visa Infinite consumer Cards and Visa Business programs

- Allow each Visa Signature Business Card account to accumulate charges of at least 10% above the approved credit limit during each billing statement cycle in which the Cardholder has satisfied previous obligations to the Issuer

ID# 0029973   **Edition: Apr 2020 | Last Updated: Apr 2020**

4.16.1.7   Visa Signature Business Card Credit Limit Non-Compliance Assessment – LAC Region

In the LAC Region: A Visa Signature Business Card Issuer that fails to meet the specified credit limit criteria is subject to a non-compliance assessment per Visa Signature Business Card in the Issuer's portfolio.

ID# 0029974   **Edition: Apr 2020 | Last Updated: Apr 2017**

4.16.2   Visa Signature Business – Customer Service Requirements

4.16.2.2   Visa Signature Business Card – Customer Service Requirements – CEMEA Region

In the CEMEA Region: A Visa Signature Business Card Issuer must:

- Provide access to a customer service and emergency telephone number 24 hours a day, 7 days a week and communicate the telephone number to the Cardholder annually
- Provide advance notification to the Cardholder when an account needs to be suspended or closed for any reason
- Monitor customer complaints related to Authorizations and make customer complaint information available to Visa
- Identify action plans to improve customer service

ID# 0029177   **Edition: Apr 2020 | Last Updated: Oct 2016**

4.16.3   Visa Signature Business – Issuer Requirements

4.16.3.6   Visa Signature Business Card Issuer Requirements – US Region

In the US Region: A Visa Signature Business Card Issuer must comply with all of the following:

- Complete the certification form
- Support Account Level Processing
- Participate in Visa SavingsEdge

ID# 0026352   **Edition: Apr 2020 | Last Updated: Apr 2019**

4.16.3.7   Visa Signature Business Card Payment Options – US Region

In the US Region: A Visa Signature Business Issuer must allow a Visa Signature Business Cardholder the option to either:

- Pay in full each statement cycle
- Revolve

ID# 0008276   **Edition: Apr 2020 | Last Updated: Oct 2014**

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

4.16.3.8   Visa Signature Business Cardholder Notification – US Region

In the US Region: A Visa Signature Business Issuer must provide notification to the Cardholder either:

- Before ongoing Transactions may be declined
- When an account needs to be suspended or closed for any reason

ID# 0004278	Edition: Apr 2020 | Last Updated: Oct 2014

4.16.4   Visa Signature Business – Features and Benefits

4.16.4.3   Visa Signature Business Cardholder Spend Reporting – CEMEA Region

In the CEMEA Region: A Visa Signature Business Card Issuer must either itself or through Visa Business Reporting, provide its Visa Signature Business Cardholders a report, at least annually, that includes both:

- Total annual amount spent by Cardholder or company
- Summary of spending by Merchant category

ID# 0029185	Edition: Apr 2020 | Last Updated: Apr 2017

4.17   Visa Infinite Business, Visa Infinite Privilege Business

4.17.1   Visa Infinite Business, Visa Infinite Privilege Business – Card Requirements

4.17.1.1   Visa Infinite Business Minimum Spending Limit – AP Region

In the AP Region: A Visa Infinite Business Card Issuer must offer one of the following spending limit options:

- No pre-set spending limit. The Issuer may establish a pre-set spending limit if the Transaction either:
  - Is a Cash Disbursement
  - Results from the use of an Emergency Card Replacement
- A Minimum Spending Limit of X (or local currency equivalent) for Transactions during each statement cycle

ID# 0029238	Edition: Apr 2020 | Last Updated: Apr 2018

4.17.1.3   Visa Infinite Business Card Point-of Sale Spend Qualification Threshold – AP Region (Australia)

In the AP Region (Australia): A Visa Infinite Business Product program must meet the average minimum annual spend requirement of AUD 200,000 at the portfolio level. If the threshold is not met, the Issuer must implement a spend stimulation program.

ID# 0029237   Edition: Apr 2020 | Last Updated: Oct 2016

4.17.1.4   Visa Infinite Business Card Account Types and Credit Limit – LAC Region

In the LAC Region: With prior approval from Visa, a Visa Infinite Business Issuer must offer the Card with credit or debit functionality.

A Visa Infinite Business Credit Card Issuer must do all of the following:

- Preserve the premium status of the Visa Infinite Business Card by providing a higher credit limit for its Visa Infinite Business program than the average credit limit for its Visa Platinum, Visa Signature, and Visa Infinite consumer cards and Visa Business programs
- Set a minimum credit limit of USD 20,000 (or local currency equivalent) or higher
- Allow each Visa Infinite Business Card account to accumulate charges of at least 20% above the approved credit limit during each billing statement cycle in which the Cardholder has satisfied previous obligations to the Issuer

ID# 0029976   Edition: Apr 2020 | Last Updated: Apr 2017

4.17.1.5   Visa Infinite Business Card Rewards Program – LAC Region

In the LAC Region: A Visa Infinite Business Issuer must provide a rewards program that:

- Offers Cardholders the ability to accumulate points for purchases made with a Visa Infinite Business Card
- Is comparable to any existing Issuer's Visa Infinite or Visa Signature rewards program

Any travel rewards program offered to the Cardholder must be sponsored by Visa (Visa rewards), the Issuer, or an Airline Affinity/Co-Brand program. The Issuer must not assess any additional fees to the Cardholder for membership in the travel rewards program.

A Visa Infinite Business debit Card Issuer is not required to offer any travel rewards programs.

ID# 0029977   Edition: Apr 2020 | Last Updated: Apr 2017

Visa Product and Service Rules

4 Issuance
Visa Core Rules and Visa Product and Service Rules

4.17.2 Visa Infinite Business, Visa Infinite Privilege Business – Customer Service Requirements

4.17.2.1 Visa Infinite Business Card Customer Service Requirements – LAC Region

In the LAC Region: A Visa Infinite Business Issuer must provide all of the following:

- Dedicated customer service 24 hours a day, 7 days a week through Visa Global Customer Care Services
- Cardholder emergency services for Visa Infinite Business Cards
- An exclusive telephone line to its Visa Infinite Business Cardholders

ID# 0029978	Edition: Apr 2020	Last Updated: Apr 2017

4.17.2.2 Visa Infinite Business Core Services and Benefits – Canada Region

In the Canada Region: A Visa Infinite Business Card Issuer must offer its Cardholders all of the benefits specified in *Section 4.1.15.2, Visa Cardholder Benefit Requirements by Product – Canada Region,* and all of the core services specified in *Section 4.12.1.3, Commercial Products Mandatory Core Services.*

ID# 0025624	Edition: Apr 2020	Last Updated: Apr 2017

4.17.3 Visa Infinite Business, Visa Infinite Privilege Business – Issuer Requirements

4.17.3.1 Use of Visa Infinite Business Product Identifier – AP and US Regions

In the AP Region, US Region[1]: A Visa Infinite Business Card Issuer must use the product identifier "Visa Infinite Business" on both:

- All statements
- All communications, including online communications, to the Cardholder regarding the Visa Infinite Business Card, except in circumstances where this poses a security risk

[1] **Effective 19 October 2019**

ID# 0029241	Edition: Apr 2020	Last Updated: Apr 2020

4.17.3.2   Visa Infinite Business Card Web Services – AP Region

In the AP Region: A Visa Infinite Business Card Issuer must, either independently or through Visa, offer its Visa Infinite Business Cardholders access to a website that offers special information and services to high-end consumers.

The Visa Infinite Business website must do all of the following:

- Limit access to Visa Infinite Business Cardholders only
- Provide a description of Visa Infinite Business Card services, benefits, and features
- Provide a detailed listing of the Visa Infinite Business Exclusive Privileges[1] offers
- Include all of the following minimum value-added content and services for travel and entertainment:
  - Travel-related content not readily available from other sources
  - Online concierge service, if concierge service is offered by the Visa Region or Member's Infinite Business product
  - Contact information for Cardholders to inquire about Visa Infinite Business services and to provide feedback

[1] A Merchant-partner program with exclusive offers for Visa Infinite Business Cardholders

ID# 0029244	Edition: Apr 2020	Last Updated: Apr 2016

4.17.3.3   Visa Infinite Business Cardholder Notification and Complaints – AP, Canada, Europe, and US Regions

Effective through 18 October 2019 In the AP Region: A Visa Infinite Business Card Issuer must both:

- Provide advance notification to the Cardholder when an account needs to be suspended or closed for any reason
- Monitor customer complaints related to Authorizations

Effective through 18 October 2019 In the Canada Region: A Visa Infinite Business Card Issuer must do all of the following:

- Provide advance notification to the Cardholder when an account needs to be suspended or closed for any reason
- Monitor customer complaints related to Authorizations
- Identify action plans to improve customer service
- Make customer complaint information available to Visa

Effective 19 October 2019 in the AP Region, Canada Region, US Region, and effective 18 July 2020 in the Europe Region A Visa Infinite Business Card Issuer must both:

- Provide advance notification to the Cardholder when an account needs to be suspended or closed for any reason
- Monitor customer complaints related to Authorizations

In the Canada Region, Europe Region[1]: In addition, a Visa Infinite Business Card Issuer must both:

- Identify action plans to improve customer service
- Make customer complaint information available to Visa

[1] **Effective 18 July 2020**

ID# 0029245	Edition: Apr 2020 | Last Updated: Apr 2020

4.17.3.4   Visa Infinite Business Card Credit Limit Non-Compliance Assessment – LAC and US Regions

In the LAC Region, US Region[1]: A Visa Infinite Business Card Issuer that fails to meet the specified credit limit criteria is subject to a non-compliance assessment per Visa Infinite Business Card in the Issuer's portfolio.

[1] **Effective 19 October 2019**

ID# 0029979	Edition: Apr 2020 | Last Updated: Apr 2020

4.17.3.5   Visa Infinite Business Card Payment Options – Canada Region

In the Canada Region: At the option of Visa, an Issuer may provide a Visa Infinite Business Card with charge and/or credit capability.

ID# 0029545	Edition: Apr 2020 | Last Updated: Apr 2017

4.17.3.6   Visa Infinite Business Card Operating Certificate Requirements – Canada Region

In the Canada Region: A Visa Infinite Business Card Issuer must complete a separate Credit Card Schedule of the Operating Certificate for reporting Visa Infinite Business Card statistics.

ID# 0029546	Edition: Apr 2020 | Last Updated: Apr 2017

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

4.17.3.7   Visa Infinite Business Card Issuer Rewards Program Requirements – Canada and Europe Regions

In the Canada Region, Europe Region[1]: A Visa Infinite Business Card Issuer must provide a rewards program to its Visa Infinite Business Cardholders with the following reward value:

- In the Canada Region: Rewards program that reasonably enables each Cardholder to redeem a minimum value equivalent to 150 basis points per dollar of qualifying spend, based on the combination of earn rates and redemption value

- **Effective 18 July 2020** In the Europe Region: Rewards program that reasonably enables each Cardholder to redeem a minimum value equivalent to 20 basis points per EUR (or local currency equivalent) of qualifying spend, based on the combination of earn rates and redemption value

- Best reward value in Issuer's Visa Business Card portfolio

- Minimum earn rate equal to or better than the rate offered by the same Issuer for a consumer Visa Infinite Card program

[1]   **Effective 18 July 2020**

ID# 0029544   Edition: Apr 2020 | Last Updated: Apr 2020

4.17.3.8   Visa Infinite Business Card Payment Options – US Region

Effective 19 October 2019 In the US Region: At the option of Visa, an Issuer may provide a Visa Infinite Business Card with charge and/or credit capability.

ID# 0030664   Edition: Apr 2020 | Last Updated: New

4.17.3.9   Visa Infinite Business Card Digital Services – Europe Region

Effective 18 July 2020 In the Europe Region: A Visa Infinite Business Card Issuer must, either independently or through Visa, offer its Visa Infinite Business Cardholders access to a platform (for example: a website or a mobile application) that shows the benefits, features, and services of the product.

ID# 0030692   Edition: Apr 2020 | Last Updated: New

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

4.17.4   Visa Infinite Business, Visa Infinite Privilege Business – Features and Benefits – AP and Canada Regions

4.17.4.1   Visa Infinite Business Card Features and Branding Requirements – AP and Canada Regions

In the AP Region, Canada Region: A Visa Infinite Business Card Issuer must offer both:

- Unique features that differentiate the Visa Infinite Business Card from any other Card it issues
- The highest purchasing power available within the Issuer's Visa Business Card suite of products

ID# 0029240	Edition: Apr 2020 | Last Updated: Apr 2020

4.17.4.3   Visa Infinite Business Card Core Features, Benefits and Services – Canada Region

In the Canada Region: A Visa Infinite Business Card Issuer must offer all of the following core features, benefits, and services:

- ATM access
- Local currency billing
- Service level standards
- Management information reporting
- POS Transaction Controls
- Limited corporate liability insurance
- Access to:
  - Visa Infinite Business concierge
  - Visa Infinite Business events and offers
  - Visa Infinite Business website

ID# 0025623	Edition: Apr 2020 | Last Updated: Apr 2017

4.17.4.4   Visa Infinite Business Web Services – Canada Region

In the Canada Region: A Visa Infinite Issuer, either itself or through other agents, must provide its Visa Infinite Cardholders website access that offers special information and services.

The Visa Infinite website service must comply with all of the following:

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

- Limit access only to Visa Infinite Cardholders

- Provide a description of Visa Infinite Card services, benefits, and features

- Provide a detailed listing of the Visa Infinite Exclusive Privileges Merchant partner offers

- Include all of the following minimum value-added content and services for travel and entertainment:

  - Travel content that supports the Visa Infinite product positioning that is not readily available from other sources (for example, special travel articles, expert recommendations on shows in major cities)

  - Online concierge service, if concierge service is offered by the Visa Region or Member's Infinite product

  - Contact information for Cardholders to inquire about Visa Infinite services and to provide feedback on the product or website

ID# 0025622	Edition: Apr 2020 | Last Updated: Oct 2014

4.17.4.5   Visa Infinite Business Issuer Rewards Program – AP Region (Australia)

In the AP Region (Australia): A Visa Infinite Business Card Issuer must provide a rewards program for its Visa Infinite Business Cardholders and must do all of the following:

- Define the rewards currency that it intends to offer

- Accrue the rewards currency to the benefit of its Cardholders for every qualifying purchase Transaction

- Ensure that the approximate retail value of services and merchandise offered for rewards redemption is comparable to the required redemption value

- Ensure that the rewards currency enables Cardholders to redeem an equivalent to 100 basis points

- Ensure that the rewards currency is accumulated for every qualifying dollar spent on the Card

- Include each purchase Transaction completed with a Visa Infinite Business Card as a qualifying purchase. The Issuer may exclude the following Transactions from qualifying for rewards currency:

  - Balance transfers

  - Convenience checks

  - Finance charges

  - Cash Disbursements

- – Quasi-Cash Transactions
  - – Fees paid to the Issuer by the Cardholder (if any)
  - – Any Transaction not authorized by the Cardholder
- Ensure that any cap on spend that earns rewards currency is not less than USD 5,000 per month or USD 60,000 per year (or local currency equivalent)
- Notify Cardholders at least quarterly of their rewards currency, including all of the following:
  - – Rewards currency earned
  - – Rewards currency redeemed
  - – Rewards currency balance remaining
  - – Upcoming rewards currency expiration, if any

If the account is no longer in good standing, the Issuer may elect to withhold rewards currency accumulation and redemption or take away currency previously accumulated.

| ID# 0029248 | Edition: Apr 2020 | Last Updated: Apr 2016 |

4.18   Visa Multi-Currency Solution

4.18.1   Visa Multi-Currency Solution Issuer Requirements

To enable Cards with the Visa Multi-Currency Solution, an Issuer's annual cross-border total volume must meet or exceed 50% of its total volume on the associated BIN or Account Range.

In addition to the requirements specified in *Section 1.4.3.2, International Transaction or Currency Conversion Fee Disclosure,* an Issuer must disclose all of the following to its Cardholders that use a Card with the Visa Multi-Currency Solution:

Table 4-21: Visa Multi-Currency Solution – Cardholder Disclosure Requirements

Disclosure Description	At Account Load	Post Transaction
Exchange rate[1] offered	X	X
Exchange rate[1] applied to Transactions[2]		X
Alternative account to be debited and exchange rate[1] applied in the event the foreign currency account has insufficient funds at the time of the Transaction (if applicable)	X	X
Associated fees	X	X

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

Table 4-21: Visa Multi-Currency Solution – Cardholder Disclosure Requirements (continued)

Disclosure Description	At Account Load	Post Transaction
Account balance per currency	X	X
Value of authorized Transactions that have not yet cleared (for example: held funds for a car rental or hotel reservation)		X
Explanation of Dynamic Currency Conversion (DCC) and impact on Transaction amount	X[3]	

[1] The Issuer must disclose the foreign exchange rate for the applicable processing date.

[2] Occurs if the Issuer elects to allow real-time conversion at the time of purchase instead of requiring funds to be loaded in a different currency in advance

[3] On initial account load only

ID# 0030592   **Edition: Apr 2020 | Last Updated: Apr 2020**

4.19   Visa SavingsEdge – US Region

4.19.1   Visa SavingsEdge Requirements – US Region

4.19.1.1   Visa SavingsEdge Requirements – US Region

In the US Region: An Issuer must offer Visa SavingsEdge to Cardholders of the following Visa products issued to small businesses:

- Visa Business Credit Cards
- Visa Business Check Cards
- Reloadable Visa Commercial Prepaid Products:
  – Visa Business Prepaid Cards
  – Visa Corporate Prepaid Cards
  – Visa Purchasing Prepaid Cards

Unless an Issuer opts out of participating in the program, Cardholders of eligible Visa products may enroll in Visa SavingsEdge in accordance with, and subject to, the program terms and conditions as revised by Visa from time to time and posted on the program Cardholder registration website.

Visa Product and Service Rules

4 Issuance

Visa Core Rules and Visa Product and Service Rules

If an Issuer opts out of the program, but its Cardholders have previously enrolled, those Cardholders will continue to remain enrolled in the program.

An Issuer that participates in the Visa SavingsEdge program must do all of the following:

- Use the program name only in connection with the Visa SavingsEdge program
- Provide customer service to handle Cardholder inquiries about the program, including questions related to credit postings
- Not opt Visa Signature Business Credit Cards out of Visa SavingsEdge participation
- Contact its Visa representative to ensure that Cardholders of Reloadable Visa Commercial Prepaid Products are enabled to enroll

For qualifying purchases made with a Visa SavingsEdge-enrolled Visa Card, an Issuer must both:

- Credit the participating Cardholder's account within 10 calendar days of receiving the Funds Disbursement from Visa
- Not alter the original Merchant name and city information posted to the Cardholder statement

ID# 0026267	Edition: Apr 2020 | Last Updated: Oct 2018

4.20   Visa Purchasing

4.20.1   Visa Purchasing – Issuer Requirements

4.20.1.1   Visa Purchasing Card Transaction Data Reporting – US Region

In the US Region: A Visa Purchasing Card Issuer must accumulate and report Transaction data and at a minimum must both:

- Match Transaction data to Merchant profiles
- Report to the Client Organization all Transactions and all Merchant profile information, both matched and unmatched

ID# 0004309	Edition: Apr 2020 | Last Updated: Oct 2014

4.20.1.2   Authorization and Settlement Match Participation Requirements

A Visa Purchasing Card Issuer choosing to participate in the Authorization and Settlement Match service must both:

- Obtain prior approval from Visa
- Enroll its Visa Purchasing Card BIN (including Visa Fleet Card BIN) or Account Range for the Authorization and Settlement Match service

ID# 0026826	Edition: Apr 2020 | Last Updated: Apr 2019

4.20.1.3   Visa Purchasing Card Selective Authorization – US Region

In the US Region: A Visa Purchasing Card Issuer may decline an Authorization Request based on the following factors if the entity to which the Card has been issued has specified these or other factors:

- MCC
- Transaction size
- Location of Merchant Outlet

ID# 0004314	Edition: Apr 2020 | Last Updated: Oct 2014

4.21   Visa Fleet

4.21.1   Visa Fleet Card – Issuer Requirements

4.21.1.1   Visa Fleet Card Requirements

A Visa Fleet Card Issuer must ensure that all of the following requirements are met:

- In the Canada Region, CEMEA Region, Europe Region: Visa Fleet Card is personalized with a Visa Fleet Card Application Identifier (AID) and a payment application that prompts for personalized data at the time of transaction
- In the Canada Region, Europe Region, US Region: Magnetic Stripe is encoded with Visa Fleet specific data that will cause a fleet-enabled terminal to prompt for personalized data at the time of Transaction
- Visa Fleet Card is issued only as one of the following:
  - A driver-assigned Visa Fleet Card
  - A Vehicle-Specific Fleet Card
  - In the LAC Region: Either a Visa Card or Visa Electron Card

In the Canada Region, CEMEA Region: A Visa Fleet Card Issuer must require the capture and/or validation of Enhanced Data by the terminal.

In the Canada Region: A Visa Fleet Card Issuer must ensure that the Chip on the Visa Fleet Card is encoded with Visa Fleet-specific data that will cause a fleet-enabled terminal to prompt for personalized data at the time of the Transaction.

In the CEMEA Region: A Visa Fleet Card Issuer must ensure that the Visa Fleet Card Chip data elements include at least both:

- Details about permitted products
- Information about the vehicle and the driver

ID# 0004168	Edition: Apr 2020 | Last Updated: Apr 2019

4.21.1.2   Visa Fleet Card Enhanced Data Requirements

A Visa Fleet Card Issuer must be capable of generating reports containing Enhanced Data when provided by the Acquirer.

ID# 0004164	Edition: Apr 2020 | Last Updated: Oct 2015

4.22   Visa Large Purchase Advantage – US Region

4.22.1   Visa Large Purchase Advantage Requirements – US Region

4.22.1.1   Visa Large Purchase Advantage Issuer Requirements – US Region

In the US Region: A Visa Large Purchase Advantage Card must comply with all of the following:

- Be issued as a Virtual Account product
- Be issued on a credit account
- Be limited to Transactions in the Commercial Payables environment that qualify as one of the following:
  - Electronic Commerce Transaction, including a Straight Through Processing Transaction
  - Mail/Phone Order Transaction
  - Recurring Transaction
  - Installment Transaction
- Not offer Cash Disbursement
- Not provide ATM access
- Unless specified otherwise, comply with the requirements applicable to Visa Purchasing Cards.

ID# 0026968	Edition: Apr 2020	Last Updated: Oct 2015

4.22.1.2   Visa Large Purchase Advantage Transaction Limitations – US Region

In the US Region: A Visa Large Purchase Advantage Transaction must comply with all of the following:

- Be processed in a Card-Absent Environment
- Not offer Cash Disbursement
- Not provide ATM access

ID# 0026969	Edition: Apr 2020	Last Updated: Oct 2017

4.23   Visa Meetings Card

4.23.1   Visa Meetings Card – Issuer Requirements

4.23.1.2   Visa Meetings Card Core Features – US Region

In the US Region: A Visa Meetings Card Issuer must provide all of the core features specified in *Section 4.12.1.2, Commercial Products Core Feature Requirements,* except for billing, where centralized company billing and payment are required.

ID# 0004335	Edition: Apr 2020	Last Updated: Oct 2014

4.23.1.3   Visa Meetings Card Authorization Processing – US Region

In the US Region: A Visa Meetings Card Issuer must have the ability to decline an Authorization Request based on the following factors, if the Client Organization has specified these or other factors:

- MCC
- Transaction amount
- Location of Merchant Outlet

ID# 0029137	Edition: Apr 2020	Last Updated: Oct 2014

4.24   Visa Infinite Corporate – LAC Region

4.24.1   Visa Infinite Corporate Card Requirements – LAC Region

4.24.1.1   Visa Infinite Corporate Card Credit Limit – LAC Region

In the LAC Region: For Visa Infinite Corporate Cards with a line of credit only, an Issuer must ensure that both:

- The minimum credit limit allowed is USD 20,000 (or local currency equivalent)

- Each Visa Infinite Corporate Card account may accumulate charges of at least 20% above the approved credit limit during each billing statement cycle in which the Cardholder has satisfied previous obligations to the Issuer

A Visa Infinite Corporate Card Issuer that fails to meet the credit limit criteria is subject to a non-compliance assessment of USD 5 per Visa Infinite Corporate Card in the Issuer's portfolio.

ID# 0027741	Edition: Apr 2020 | Last Updated: Apr 2015

4.24.1.2   Visa Infinite Corporate Card Spending Limits – LAC Region

In the LAC Region: A Visa Infinite Corporate Card Issuer must offer either of the following spending limit options:

- No pre-set limit

- Minimum limit allowing each Visa Infinite Corporate Card account to accumulate charges of at least USD 20,000 (or local currency equivalent) during each or any statement cycle in which a Cardholder has satisfied previous obligations to the Issuer

Visa may impose additional restrictions to these options.

ID# 0027742	Edition: Apr 2020 | Last Updated: Apr 2019

4.24.2   Visa Infinite Corporate – Issuer Requirements – LAC Region

4.24.2.1   Visa Infinite Corporate Card Benefit Notification – LAC Region

In the LAC Region: A Visa Infinite Corporate Card Issuer offering benefits in addition to those provided through Visa must provide Visa with all necessary information concerning those benefits and the benefit providers on a quarterly basis.

ID# 0027747	Edition: Apr 2020 | Last Updated: Oct 2014

4.24.2.2   Visa Infinite Corporate Card Declined Authorizations – LAC Region

Effective through 18 April 2020 In the LAC Region: An Authorization response code 05 (Authorization Declined) may be generated for a Visa Infinite Corporate Card Authorization Request only if both the:

- Account is delinquent, for at least a second time

- Transaction is an ATM Cash Disbursement that both:

    – Exceeds Issuer activity parameters

    – Received a response by Stand-In Processing through an Issuer's Positive Authorization Capacity Management Service

ID# 0027749	Edition: Apr 2020 | Last Updated: Oct 2019

4.24.2.3   Visa Infinite Corporate Card Declined Transactions – LAC Region

In the LAC Region: For Visa Infinite Corporate Cards issued with a no preset limit, the Issuer must provide notification to the Cardholder before ongoing Transactions can be declined.

Visa Infinite Corporate Card Authorization Requests must only be declined with response code 51 (Not Sufficient Funds) if either:

- The Transaction places the account balance more than 20% above the approved line of credit

- The Transaction is for an ATM Cash Disbursement that exceeds activity parameters and is responded to by the Issuer

ID# 0027743	Edition: Apr 2020 | Last Updated: Oct 2014

4.24.2.4   Visa Infinite Corporate Card Issuer Certification – LAC Region

In the LAC Region: Before issuing a Visa Infinite Corporate Card an Issuer must receive written certification from Visa that the Issuer complies with all Visa Infinite Corporate product requirements and standards.

ID# 0027739	Edition: Apr 2020 | Last Updated: Oct 2014

4.24.2.5   Visa Infinite Corporate Card Issuer Processing System Requirement – LAC Region

In the LAC Region: A Visa Infinite Corporate Card Issuer or its agent must demonstrate that its processing system has the minimum capacities to meet the standards for processing Authorizations

regarding Visa Infinite Cards and Visa Corporate Cards.

ID# 0027746	Edition: Apr 2020 | Last Updated: Apr 2020

4.24.3   Visa Infinite Corporate – Features and Benefits – LAC Region

4.24.3.1   Visa Infinite Corporate Card Features and Branding Requirements – LAC Region

In the LAC Region: A Visa Infinite Corporate Card Issuer must offer both:

- Unique features that differentiate the Visa Infinite Corporate Card from any other Card product it issues
- The highest purchasing power available within the LAC Region and an Issuer's Card portfolio, except when the Member-developed Card product:
  - Is not branded with a Card product name
  - Does not use the Sample Card Design or reserved color of a Card product

ID# 0027740	Edition: Apr 2020 | Last Updated: Apr 2020

4.25   Visa Platinum Corporate – LAC Region

4.25.1   Visa Platinum Corporate – Card Requirements – LAC Region

4.25.1.1   Visa Platinum Corporate Card Credit Limit – LAC Region

In the LAC Region: For Visa Platinum Corporate Cards with a line of credit only, a Visa Platinum Corporate Issuer must both:

- Ensure that the average credit limit for its Visa Platinum Corporate program must be higher than the average credit limit for its Visa Platinum and Visa Corporate programs
- Allow each Visa Platinum Corporate Card account to accumulate charges of at least 10% above the approved credit limit during each billing statement cycle in which the Cardholder has satisfied previous obligations to the Issuer

A Visa Platinum Corporate Card Issuer that fails to meet the credit limit criteria is subject to a non-compliance assessment per Visa Platinum Corporate Card in the Issuer's portfolio.

ID# 0027738	Edition: Apr 2020 | Last Updated: Oct 2014

4.25.2   Visa Platinum Corporate Issuer Requirements – LAC Region

4.25.2.1   Visa Platinum Corporate Card Issuer Certification – LAC Region

In the LAC Region: Before issuing a Visa Platinum Corporate Card an Issuer must receive written certification from Visa that the Issuer complies with all Visa Platinum Corporate product requirements and standards.

ID# 0027736	Edition: Apr 2020 | Last Updated: Oct 2014

4.25.3   Visa Platinum Corporate Features and Benefits – LAC Region

4.25.3.1   Visa Platinum Corporate Card Benefits – LAC Region

In the LAC Region: A Visa Platinum Corporate Issuer offering benefits in addition to those provided through Visa must provide Visa with all necessary information concerning those benefits and the benefit providers.

ID# 0027737	Edition: Apr 2020 | Last Updated: Oct 2014

4.26   Visa Premium Corporate – LAC Region

4.26.1   Visa Premium Corporate – Issuer Requirements – LAC Region

4.26.1.1   Visa Premium Corporate Cards Core Product Benefits – LAC Region

In the LAC Region: A Visa Premium Corporate Issuer must provide its Visa Premium Corporate Cardholders with all of the following core product benefits, unless prohibited by applicable laws or regulations:

Table 4-22: Visa Premium Corporate Card Core Product Benefits – LAC Region

Core Product Enhancements	Visa Platinum Corporate	Visa Signature Corporate	Visa Infinite Corporate
Visa Global Customer Assistance Services	Global	Global	Global
Travel Accident Insurance	USD 500,000	USD 1,000,000	USD 1,500,000
Auto Rental Insurance	Global	Global	Global
Visa International Emergency Medical	Plan Platinum up to	Plan Infinite up to	Plan Infinite up to

Table 4-22: Visa Premium Corporate Card Core Product Benefits – LAC Region (continued)

Core Product Enhancements	Visa Platinum Corporate	Visa Signature Corporate	Visa Infinite Corporate
Services	USD 150,000	USD 200,000	USD 200,000
Insured Journey/24 Hour AD&D	USD 25,000	USD 50,000	USD 100,000
Visa Concierge	Global	Global	Global
Baggage Delay	USD 0	USD 500	USD 600
Baggage Loss	USD 750	USD 1,000	USD 3,000
Trip Delay	USD 0	USD 0	USD 300
Trip Cancellation	USD 0	USD 0	USD 3,000
Missed Connection	USD 0	USD 0	USD 2,000
Hotel Burglary $1000	USD 0	USD 500	USD 1,000
Priority Pass	Optional	Optional	Yes
Corporate Liability Waiver Insurance (CLW)	USD 15,000	USD 15,000	USD 15,000
ATM Assault–Coverage in case of Death	USD 0	USD 0	USD 10,000
ATM Assault–Cash Stolen	USD 0	USD 0	Up to USD 3,000
Program Membership Rewards	Optional	Optional	Optional
Visa Luxury Hotel Collection	Global	Global	Global

ID# 0027727   Edition: Apr 2020 | Last Updated: Oct 2016

4.26.1.2   Visa Premium Corporate Cards Customer Service Requirements – LAC Region

In the LAC Region: A Visa Premium Corporate Issuer must do all of the following:

- Provide Customer service 24 hours a day, 7 days a week
- Provide Cardholder emergency services for Visa Platinum, Visa Infinite, or Visa Signature

- Respond to a Visa Premium Corporate Cardholder with a live operator

- Provide an exclusive telephone line to its Visa Premium Corporate Cardholders

Assistance must be provided in English, Portuguese, and Spanish through Visa Global Customer Care Services.

ID# 0027726	Edition: Apr 2020 | Last Updated: Oct 2014

4.26.1.3   Visa Premium Corporate Cards Emergency Services – LAC Region

In the LAC Region: A Visa Premium Corporate Card Issuer must offer customer support services required for Visa Corporate Cards.

ID# 0027730	Edition: Apr 2020 | Last Updated: Oct 2014

4.26.1.4   Visa Premium Corporate Cards Issuance Requirements – LAC Region

In the LAC Region: An Issuer of Visa Premium Corporate Cards must do all of the following:

- Comply with the requirements for Visa Corporate Cards and *Section 4.26.1, Visa Premium Corporate – Issuer Requirements – LAC Region*

- Issue Visa Premium Corporate Cards as any of the following:

  - Visa Platinum Corporate

  - Visa Infinite Corporate

  - Visa Signature Corporate

- Issue Visa Premium Corporate Cards with credit, debit, or charge capability

ID# 0027724	Edition: Apr 2020 | Last Updated: Oct 2014

4.26.1.5   Visa Premium Corporate Cards Mandatory Core Features – LAC Region

In the LAC Region: A Visa Premium Corporate Card Issuer must provide the core features required for Visa Corporate Cards.

ID# 0027729	Edition: Apr 2020 | Last Updated: Oct 2014

4.26.1.6   Visa Premium Corporate Cards Mandatory Core Services – LAC Region

In the LAC Region: A Visa Premium Corporate Card Issuer must offer customer support services required for Visa Corporate Cards.

ID# 0027728   Edition: Apr 2020 | Last Updated: Oct 2014

4.26.1.7   Visa Premium Corporate Cards Performance Standards – LAC Region

In the LAC Region: A Visa Premium Corporate Card Issuer that exceeds the Negative Authorization Response standard of 2% as a percentage of its total Authorization Responses in a calendar month is subject to a non-compliance assessment for each Negative Authorization Response exceeding the standard. A Negative Authorization Response is any Authorization that is not an Approval Response.

A Visa Premium Corporate Card Issuer that fails to meet the performance standard specified in this section is subject to corrective action. Fees double each calendar month of the de-certification period, as follows:

Table 4-23: Corrective Actions for Issuer Failure to Meet Performance Standards for Visa Premium Corporate Cards – LAC Region

Stage	Action/Response
Grace Period – One calendar month (begins the calendar month following the first violation for under-performance)	Written notification of under-performance and recommended corrective actions
Observation Period – Two calendar months (begins at completion of Grace Period)	• Fees imposed as specified above • Member has 2 calendar months to apply corrective actions
Probation Period – Three calendar months (begins at completion of Observation Period)	• Fees imposed as specified above • Visa may audit Member at Member's expense
De-certification Period - Begins at completion of Probation Period	• Member prohibited from issuing or reissuing Visa Premium Corporate Cards • Fees imposed and doubled for each calendar month as specified above • Visa reserves its right to resolve Authorization Requests via the PCAS-Full Service system

ID# 0027734   Edition: Apr 2020 | Last Updated: Oct 2014

4.26.1.8   Visa Premium Corporate Cards Reporting Requirements – LAC Region

In the LAC Region: A Visa Premium Corporate Issuer must report its Visa Premium Corporate Card activity separately through the Operating Certificate.

ID# 0027731	Edition: Apr 2020	Last Updated: Oct 2014

4.27   Visa Signature Corporate – LAC Region

4.27.1   Visa Signature Corporate Issuer Requirements – LAC Region

4.27.1.1   Visa Signature Corporate Card Benefit Notification – LAC Region

In the LAC Region: A Visa Signature Corporate Card Issuer offering benefits in addition to those provided through Visa must provide Visa with all necessary information concerning those benefits and the benefit providers on a quarterly basis.

ID# 0027753	Edition: Apr 2020	Last Updated: Oct 2014

4.27.1.2   Visa Signature Corporate Card Credit Limit and Spending Limits – LAC Region

In the LAC Region: An Issuer of Visa Signature Corporate Card must issue Visa Signature Corporate cards without a pre-set spending limit

The Visa Signature Corporate Card Issuer must ensure that the average credit limit for its Visa Signature Corporate Card program is higher than the average credit limit for its Visa Signature and Visa Corporate programs.

A Visa Signature Corporate Issuer that fails to meet the credit limit criteria is subject to a non-compliance assessment per Visa Signature Corporate Card in the Issuer's portfolio.

ID# 0027752	Edition: Apr 2020	Last Updated: Oct 2014

4.27.1.3   Visa Signature Corporate Card Issuer Certification – LAC Region

In the LAC Region: Before issuing a Visa Signature Corporate Card an Issuer must receive written certification from Visa that the Issuer complies with all Visa Signature Corporate product requirements and standards.

ID# 0027751	Edition: Apr 2020	Last Updated: Oct 2014

4.28   Prepaid Commercial Corporate

4.28.1   Commercial Prepaid – Card Requirements

4.28.1.1   Visa Commercial Prepaid Product Requirements

A Visa Commercial Prepaid Product Issuer must comply with the Prepaid Card requirements and general Visa Commercial Card requirements.

ID# 0025575	**Edition: Apr 2020 | Last Updated: Apr 2020**

4.28.2   Corporate Prepaid – Features and Benefits

4.28.2.1   Visa Corporate Prepaid Card – Commercial Products Core Feature Requirements

In addition to the Visa Commercial Card core features specified in *Section 4.12.1.2, Commercial Products Core Feature Requirements,* for Visa Corporate Cards, a Visa Corporate Prepaid Card Issuer must support all of the following:

- Individual memo statements
- Personalized and non-personalized Cards
- Domestic use only Transaction Authorization
- Load and Transaction limits
- Instant Card issuance
- Multiple currencies
- Online Cardholder statements
- Program administration services

ID# 0026738	**Edition: Apr 2020 | Last Updated: Oct 2014**

4.29   Visa Agro – LAC Region

4.29.1   Visa Agro – Card Requirements – LAC Region

4.29.1.1   Visa Agro Issuer Requirements – LAC Region

In the LAC Region: An Issuer of Visa Commercial Cards may issue a Visa Agro Card as any of the following:

- Credit
- Debit
- Prepaid commercial, excluding Cards issued in Brazil
- Visa Electron

The Issuer may combine Visa Agro Cards with the commercial applications or commercial products described above.

Visa Agro Card Issuers must comply with the regulations of each product and application associated with the Visa Agro Card.

ID# 0026520	Edition: Apr 2020	Last Updated: Oct 2014

4.29.2   Visa Agro – Customer Service Requirements – LAC Region

4.29.2.1   Visa Agro Card Core Services – LAC Region

In the LAC Region: A Visa Agro Card Issuer must offer both:

- Visa Global Customer Assistance Services, as specified in *Section 4.1.14.5, Visa Global Customer Assistance Services Provision Requirements*
- Free 24-hour telephone number to obtain emergency services

For Visa Agro Cards issued as Visa Commercial Prepaid Products, Issuers must offer the customer support services for Prepaid Cards, as specified in *Section 4.1.14.5, Visa Global Customer Assistance Services Provision Requirements*.

ID# 0026523	Edition: Apr 2020	Last Updated: Apr 2020

4.29.3   Visa Agro – Issuer Requirements – LAC Region

4.29.3.1   Visa Agro Card Selective Authorization – LAC Region

In the LAC Region: A Visa Agro Card Issuer may decline an Authorization Request based on any of the following factors, if the Client Organization has specified these or other factors:

- Merchant Category Code
- Transaction amount
- Location of Merchant Outlet

ID# 0026524	Edition: Apr 2020 | Last Updated: Oct 2014

4.30   Visa Cargo – LAC Region

4.30.1   Visa Cargo Card Requirements – LAC Region

4.30.1.1   Visa Cargo Issuer Requirements – LAC Region

In the LAC Region: An Issuer may issue a Visa Cargo Card as either:

- Visa Commercial Prepaid Product
- Visa Business Electron Card

Visa Cargo Card Issuers must comply with the regulations of each product and application associated with the Visa Cargo Card.

ID# 0025631	Edition: Apr 2020 | Last Updated: Oct 2015

4.30.1.2   Visa Cargo Core Benefits – LAC Region

In the LAC Region: A Visa Cargo Card Issuer must provide its Visa Cargo Cardholders with all of the following core product benefits, unless prohibited by applicable laws or regulations:

- Visa Global Customer Assistance Services, as specified in *Section 4.1.14.5, Visa Global Customer Assistance Services Provision Requirements*
- 24 Hours Accident Protection with a coverage amount of USD 1,000 (or local currency equivalent)
- ATM Assault (Cash Stolen) with a coverage amount of USD 100 (or local currency equivalent)

ID# 0029273	Edition: Apr 2020 | Last Updated: Apr 2019

4.31 Visa Drive Card – Europe Region

4.31.1 Visa Drive Card – Europe Region

4.31.1.1 Visa Drive Card Issuer Requirements – Europe Region

In the Europe Region: A Visa Drive Card Issuer must comply with all of the following

Table 4-24: Visa Drive Card Requirements – Europe Region

Element	Requirement
Payment Device	May be any of the following: • A physical Card • A Contactless Chip Card • A Contactless Payment Device • A Virtual Account
Types	May be one or more of the following: • "Standard" Card • "Extra" Card • "Open" Card
Issuance	May be issued to either: • One Cardholder • A specific vehicle, which may have multiple individuals associated with it
BINs	• An "open" Card must be issued on a dedicated BIN. • A "standard" Card and an "extra" Card may be issued on the same BIN, but each Card must have a dedicated Account Range. • Cards that are issued to a Cardholder and Cards that are issued to a specific vehicle must be issued on separate Account Ranges within the same BIN.
Data	Must provide Visa with Visa-specified data for Visa Drive Card Transactions upon Visa request
PIN Changes	Must provide the capability for a Cardholder or an authorized individual to change a PIN at an ATM.

Table 4-24: Visa Drive Card Requirements – Europe Region (continued)

Element	Requirement

"Standard" Card Requirements	• Must ensure that the Card is configured to be used only in a Closed Loop
	• Must provide the Cardholder with terms and conditions including, but not limited to:
	  – Using the Card at a Point-of-Transaction Acceptance Device inside the Closed Loop for that Issuer
	  – PIN management

"Extra" Card Requirements	• Must comply with general requirements for Visa Commercial Cards
	• Must ensure that the Card is configured to be used only at Point-of-Transaction Acceptance Devices:
	  – Within a Closed Loop
	  – With a Merchant with which the Issuer has a Privately Contracted Agreement
	• For a Transaction at a Merchant with whom the Issuer has a Privately Contracted Agreement, must request Online Authorization, except for the following MCCs:
	  – 4784 (Tolls and Bridge Fees)
	  – 7523 (Parking Lots, Parking Meters and Garages)
	• Must provide evidence of Privately Contracted Agreements upon Visa request
	• Is solely responsible for the management of a Privately Contracted Agreement
	• Must provide the Cardholder with terms and conditions including, but not limited to:
	  – Prohibition of the use of the Card at any Point-of-Transaction Acceptance Device outside the Closed Loop if the Issuer does not have a Privately Contracted Agreement with the Merchant
	  – PIN management

"Open" Card Requirements	• Must comply with general requirements for Visa Commercial Cards • Must comply with the core feature requirements for the Card it is licensed to issue

Table 4-24: Visa Drive Card Requirements – Europe Region (continued)

Element	Requirement
	• Must provide the Cardholder with terms and conditions including, but not limited to: – The Cardholder Verification Method (CVM) allowed for a Card issued for a specific vehicle – PIN management

ID# 0029637	Edition: Apr 2020 | Last Updated: Apr 2019

4.32   Visa SimplyOne – Europe Region

4.32.1   Visa SimplyOne Card – Europe Region

4.32.1.1   Visa SimplyOne Card Issuer Requirements – Europe Region

In the Europe Region: A Visa SimplyOne Card Issuer must comply with all of the following:

- Issue the Card as a Visa Card or Visa Electron Card[1]
- Issue the Card with 2 Payment Credentials, which must both:
    - Be issued by the same Issuer
    - Be associated with the Payment Application(s) encoded on the Chip and the Magnetic Stripe. One Payment Application must be the Visa Higher Priority Payment Application. Any other Payment Application will be classified as a Visa Lower Priority Payment Application.
- If issued as a Contactless Chip Card, have the Contactless payment associated to the Visa Higher Priority Payment Application[2]
- Issue the Payment Application on a designated BIN, as follows:
    - The debit application on a Debit Card BIN
    - The credit application on a Credit Card BIN
    - The consumer application on a Visa Consumer Card BIN
    - The commercial application on a Visa Commercial Card BIN
- Comply with debit rules when the Card is used as a Debit Card and credit rules when the Card is used as a Credit Card

- Not issue a Non-Reloadable Prepaid Card when the Card is used as a Prepaid Card

- Stop or close both accounts in order to stop or close the Card

[1]   In the Europe Region (Republic of Ireland, United Kingdom): An Issuer must not issue a Visa Electron Card.

[2]   This does not apply in the Europe Region (Finland), where the Issuer may associate the Contactless payment to the Visa Lower Priority Payment Application only if it clearly communicates to its Cardholders that the Visa Lower Priority Payment Application must be selected after the maximum number of cumulative offline Transactions has been reached.

ID# 0029639	Edition: Apr 2020 | Last Updated: Apr 2020

4.33   Visa Multichoice – Europe Region

4.33.1   Visa Multichoice Card – Europe Region

4.33.1.1   Visa Multichoice Card Issuer Requirements – Europe Region

In the Europe Region: An Issuer of a Visa Multichoice Card must ensure all of the following:

- The Card supports 2 or more Payment Applications on the same account

- All the Payment Applications on the Card are issued by the same Issuer using the same Payment Credential

- One of the Payment Applications is encoded as the Visa Higher Priority Payment Application on the Chip and Magnetic Stripe

- The Payment Applications must be either consumer credit or business credit

- A Contactless Transaction must be associated with the Visa Higher Priority Payment Application

- The Card is issued on a Credit Card BIN

- The "Issuer Discretionary Data" field in the Chip is used to distinguish between the Payment Applications

- Consumer Credit and Business Credit Payment Applications are not combined on a Card

ID# 0029640	Edition: Apr 2020 | Last Updated: Apr 2020

4.34   Carte Bleue Nationale Cards – Europe Region

4.34.1   Carte Bleue Nationale Cards Issuer Requirements – Europe Region (France)

4.34.1.1   Carte Bleue Nationale Cards Issuer Requirements – Europe Region (France)

In the Europe Region (France): A Carte Bleue Nationale Card Issuer (including Cards with systematic authorization) must comply with *Table 4-25, Service Requirements for France Domestic Transactions using Carte Bleue Nationale Cards*.

Table 4-25: Service Requirements for France Domestic Transactions using Carte Bleue Nationale Cards

Card Type	Cash Withdrawal Services	Payment Services in Card-Present Environment	Payment Services in Card-Absent Environment	Travel Insurance [1]	Medical Insurance [1]	Welcome Pack [2]	Concierge Services
Carte Bleue Nationale	X	X	X				
Carte Bleue Nationale (with systematic authorization)	X	X					
Visa Electron	X	X					
Visa Classic	X	X	X	X [3]	X [3]		
Visa Premier	X	X	X	X	X		
Visa Platinum	X	X	X	X	X	X	X
Visa Infinite	X	X	X	X	X	X	X
[1] As specified in the corresponding terms and conditions							
[2] Must include the contract and the associated services							
[3] For personal trips only; for medical insurance, only international trips							

ID# 0030094	Edition: Apr 2020 | Last Updated: Oct 2017

4.35   Carte Bleue Nationale Affaires Cards – Europe Region (France)

4.35.1   Carte Bleue Nationale Affaires Cards Issuer Requirements – Europe Region (France)

4.35.1.1   Carte Bleue Nationale Affaires Cards Issuer Requirements – Europe Region (France)

In the Europe Region (France): An Issuer must comply with all of the following:

- A Visa Affaires Card Issuer must use a Visa Corporate Card BIN

- A Plus Card Issuer must issue this as a Debit Card

- A Carte Bleue Nationale Affaires Card Issuer must comply with *Table 4-26, Service Requirements for France Domestic Transactions using Carte Bleue Nationale Affaires Cards*

Table 4-26: Service Requirements for France Domestic Transactions using Carte Bleue Nationale Affaires Cards

Card Type	Cash Withdrawal Services	Payment Services in Card-Present Environment	Payment Services in Card-Absent Environment	Travel Insurance[1]	Medical Insurance[1]	Welcome Pack[2]	Concierge Services
Visa Affaires	X	X	X	X[3]	X[4]		
Visa Gold Affaires	X	X	X	X[5]	X[5]		
Visa Business Electron	X	X		X[6]	X[4]		
Carte Plus	X						
Carte Bleue Nationale Business	X	X	X	X[6]			

Table 4-26: Service Requirements for France Domestic Transactions using Carte Bleue Nationale Affaires Cards (continued)

Card Type	Cash Withdrawal Services	Payment Services in Card-Present Environment	Payment Services in Card-Absent Environment	Travel Insurance[1]	Medical Insurance[1]	Welcome Pack[2]	Concierge Services
Visa Business	X	X	X	X[6]	X[4]	X	
Visa Gold Business	X	X	X	X[7]	X[7]	X	
Visa Platinum Business	X	X	X	X[7]	X[7]	X	X

[1] Must be in accordance with the corresponding terms and conditions

[2] Must include the contract and the associated services

[3] For professional trips only (EUR 100,000 allowance)

[4] Overseas travel only (EUR 11,000 allowance)

[5] For professional trips only

[6] EUR 46,000 allowance for personal trips, EUR 100,000 allowance for professional trips

[7] All types of trips (one staff member)

ID# 0030095   Edition: Apr 2020 | Last Updated: Apr 2020

5   Acceptance

5.1   Responsibilities Related to Information and Notification

5.1.1   Provision of Information, Registration, and Reporting

5.1.1.1   Provision of Required Merchant Information

In a Visa Region where the collection of Merchant data is required, an Acquirer or its Agent must provide to Visa the following information for each Merchant, Marketplace, Sponsored Merchant, or retailer signed by a Staged Digital Wallet Operator, or retailer signed by a Marketplace. The information must be accurate, updated whenever the information changes, and in the format specified by Visa.

- T/A (trading as) or DBA (doing business as) name

- Full legal name (if different from DBA name). For a sole proprietor, the information must include the sole proprietor's full first and last name, including the middle initial.

- Merchant Outlet address (including street address, city, state/province, and postal code [or country equivalent])[1]

- Telephone number (not required for Sponsored Merchants)[2]

- Acquirer-assigned Merchant ID

- Card acceptor identification[3]

- Merchant business registration number or tax identification number[4]

- Payment Facilitator name (for Sponsored Merchants only)

- Payment Facilitator identifier assigned by Visa and Sponsored Merchant identifier assigned by the Payment Facilitator, as applicable

- In the AP Region: In addition, the Acquirer must submit monthly the Merchant data using the acquirer merchant master file format.

- In the CEMEA Region, Europe Region: In addition, the Acquirer must submit monthly the Merchant data using the acquirer merchant master file format.

- In the Canada Region: In addition:

  – The Acquirer must submit monthly, the Merchant data using the acquirer merchant master file format.

  – The Merchant name, Card acceptor identification, and terminal identification for each Acceptance Device at the Merchant Outlet, as they appear in the Clearing Record

- – The unique identifier for each acceptor device sharing one terminal identification

- – The Merchant's chain identification and Merchant identification, if different from the Merchant's Card acceptor identification (optional as appropriate)

- – Seasonality indicator (if applicable)

- – An indication of whether the Merchant:

  - ▪ Sells online or via mail order/telephone order

  - ▪ Is a Visa Debit Acceptor

  - ▪ Accepts Visa Contactless payments

- – An indication of the terminal (if available):

  - ▪ Contactless version

  - ▪ Whether it is a mobile POS (mPOS)

  - ▪ Capabilities: magnetic stripe, Chip, and/or Visa Contactless

- – The Merchant's primary and any secondary MCCs

- – If the Acquirer/Merchant relationship has been terminated, the termination date and reason for termination

- In the LAC Region: In addition:

  - – The Acquirer must submit monthly, the Merchant data using the acquirer merchant master file format.

  - – In Brazil: An Acquirer must obtain consent from a Payment Facilitator to send Merchant data. If not, the Payment facilitator must send the Merchant data directly to Visa.

- In the US Region: In addition:

  - – Merchant's incorporation status (for example: corporation, partnership, sole proprietor, non-profit)

  - – Merchant's primary and any secondary MCCs

  - – If the Acquirer/Merchant relationship has been terminated, the termination date and reason for termination

In the US Region: An Acquirer must provide to Visa monthly notification of all new Contactless Acceptance Device deployments.

[1] In the US Region: The 9-digit zip code

[2] In the Canada Region: This does not apply.

[3] For Sponsored Merchants, the Payment Facilitator's Card acceptor identification is acceptable.

---

⁴ In the US Region: The US Federal Taxpayer Identification Number, and identification of the number as either a US Federal Employer Identification Number (FEIN) or Social Security Number (SSN)

ID# 0026460	Edition: Apr 2020 | Last Updated: Apr 2020

5.1.1.3   Acquirer Compliance with Privacy Legislation – Canada Region

In the Canada Region: An Acquirer must meet all applicable requirements of privacy legislation for the collection, use, and disclosure of personal information among Visa and its employees and agents, for the purpose of a Merchant's participation in the Visa Program.

ID# 0005395	Edition: Apr 2020 | Last Updated: Oct 2014

5.1.1.4   Visa Drive Card – Merchant Requirement for "Extra" Cards – Europe Region

In the Europe Region: If a Merchant establishes a Privately Contracted Agreement with an Issuer, the Merchant must notify its Acquirer.

ID# 0029638	Edition: Apr 2020 | Last Updated: Oct 2016

5.2   Acquirer Responsibilities Related to Merchants

5.2.1   Merchant Agreements, Merchant Onboarding, and Merchant Relationships

5.2.1.1   Requirements for Acquirers Soliciting Electronic Commerce Merchant Applications

An Acquirer soliciting Merchant applications must list Merchant Outlet location requirements on its website and/or application.

ID# 0004630	Edition: Apr 2020 | Last Updated: Apr 2017

5.2.1.2   Due Diligence Review of Prospective Merchant or Sponsored Merchant

Before contracting with a prospective Merchant or Sponsored Merchant, an Acquirer or a Payment Facilitator must conduct an adequate due diligence review, including a site visit to the business premises (if applicable) or suitable alternative, to ensure compliance with the Acquirer's obligation to submit only legal Transactions to VisaNet.

ID# 0005251	Edition: Apr 2020 | Last Updated: Apr 2018

5.2.1.3   Acquirer Monitoring of Merchant Bankruptcy or Regulatory Proceedings – US Region

In the US Region: An Acquirer that becomes aware of the potential or actual bankruptcy of, or any regulatory proceedings involving, its Merchants must both:

- Notify Visa no later than close of business on the next business day following such discovery
- Oppose to the best of its ability any request for legal relief that would interfere with the Dispute process

ID# 0029138	Edition: Apr 2020	Last Updated: Apr 2018

5.2.1.5   Terminated Merchant File Query – US Region

In the US Region: An Acquirer must query the Terminated Merchant File before entering into a Merchant Agreement with a prospective Merchant.

If the Acquirer receives a response indicating a possible match to a Merchant listed on the Terminated Merchant File, the Acquirer must both:

- Verify that the Merchant identified in the response is the same Merchant for which the inquiry was generated
- Contact the listing Member directly to determine why the Merchant was added to the file

The Acquirer must use Terminated Merchant File data only as an informational tool in the decision-making process.

ID# 0008577	Edition: Apr 2020	Last Updated: Oct 2014

5.2.1.6   Acquirer Allowance of Terminal Processing by Competitors – US Region

In the US Region: An Acquirer must not prohibit a Merchant from using terminal processing services offered by competitors for the direct delivery of Visa Transactions captured at the Point-of-Transaction to VisaNet for Clearing and Settlement.

ID# 0003362	Edition: Apr 2020	Last Updated: Oct 2014

5.2.1.7   Additional Merchant Agreement Requirements

In addition to the requirements in *Section 1.5.2.1, Merchant Agreement Requirements,* a Merchant Agreement must comply with all of the following:

- For International Airline Program participants, both:
    - List the countries from which the Acquirer will accept Transactions
    - Require the Merchant to comply with all laws and regulations, and Visa Rules, applicable to each Merchant Outlet and Merchant country
- In the Canada Region: For a Merchant that has elected to be a Visa Debit Acceptor, both:
    - Identify Card acceptance-related fees associated with Visa Debit Category Acceptance
    - For an existing Merchant Agreement that is renewed, or if the Merchant indicates to its Acquirer that it wants to accept Visa Debit Category Cards, be revised to include the Merchant's option to be a Visa Debit Acceptor and identify all Card acceptance-related fees
- In the Europe Region: All of the following:
    - Specify that the Merchant must not misrepresent itself as being a Member
    - Include all information required under applicable data protection legislation, including, but not limited to, the following:
        - The identity of the Acquirer
        - The purposes of the processing for which any Personal Data is intended
        - The recipients of the Personal Data, such as:
            - Member's subsidiaries and/or group of companies, agents, and employees
            - Visa, its employees, and its third-party subcontractors and their employees
            - Such other entities to which it may be reasonably necessary to disclose and transfer Personal Data (for example: credit reference agencies, law enforcement agencies, anti-terrorism or organized crime agencies, fraud monitoring agencies, central banks)
            - Any other entities, to be clearly specified, as otherwise required or permitted by applicable laws or regulations
        - That the transfer and disclosure of Personal Data may take place worldwide and that the transfer of Personal Data outside the EEA is on the basis of either:
            - An adequacy decision by the European Commission
            - Appropriate or suitable safeguards as required by applicable laws or regulations

            Where the basis of a transfer is for appropriate or suitable safeguards, the Member is responsible for ensuring that Merchants can have access to such appropriate or suitable safeguards.
        - Any other information necessary to guarantee fair processing of Personal Data under applicable laws or regulations, including without limitation:

- That aggregated, anonymized data may be created based on Personal Data

- That data may be used and/or shared where deemed applicable with third parties for:

  - Billing purposes

  - Product enablement and build

  - Testing or product improvement purposes

  - To reply to requests from public authorities

- That data subjects are not identifiable from this data

- The categories of Personal Data processed, whenever considered necessary for the legitimate interests pursued by the Member

- A contact point for data protection enquiries and/or subject access requests

– Notify the Merchant that Merchant Service Charge (MSC) pricing on a MIF Plus Plus basis is available for Transactions completed with a consumer credit Card or consumer debit Card and specify the amount of any administrative fee charged by the Acquirer for this service

– Specify the amount of the MSC, Interchange Reimbursement Fees (IRF), and scheme fees applicable for each Visa Product Category, unless the Merchant requests in writing that the pricing information be provided in a different format

– Not blend MSCs between Visa Transactions and the transactions of other payment schemes, unless specifically requested to do so by the Merchant

– For an Electronic Commerce Transaction processed using Visa Secure, include the Issuer or Visa-provided Cardholder Authentication Verification Value in an Authorization Request

– Specify that the Merchant must undertake PIN Entry Device asset management on a regular basis, including all of the following:

  - Recording all stock and serial numbers of each PIN Entry Device

  - Recording the location of each PIN Entry Device

  - Undertaking basic electronic and physical identification, and authentication of each PIN Entry Device

– That both the Acquirer and Merchant shall ensure that all staff are appropriately trained in line with their responsibilities under applicable data protection law.

– In addition, where the Member is located in the EEA and the Merchant, also located in the EEA, is a sole trader, all of the following:

  - The identity of the Acquirer as data controller and corresponding contact details

  - The identity of any additional data controller and corresponding contact details

- ▪ Identity and contact details for the appropriate data protection officer

- ▪ The legitimate interest of the data controller where any processing is based on such interest

- ▪ The data storage period or, where not specific, the criteria used to determine that period

- ▪ All data rights available to the Merchant, taking into account the relevant Visa services, including the right to lodge a complaint with an authority and, where applicable, the right to erasure and/or correction of Personal Data and data portability

- In the US Region: All of the following:

  - – Clearly distinguish fees associated with Transactions from fees associated with non-Visa transactions

  - – Clearly and obviously specify all of the following:

    - ▪ The Acquirer's name and location

    - ▪ The terms of payment to the Merchant

    - ▪ The Acquirer's responsibilities, if an Agent is a party to the Merchant Agreement

  - – For new or renewed Merchant Agreements, both:

    - ▪ Specify the Limited Acceptance options and the Merchant's election, if any, of one of those options

    - ▪ Distinguish all Card acceptance-related fees, such as discount rates or other pricing methodology, associated with each Limited Acceptance category

  - – Provide for the immediate termination of a Merchant for any significant circumstances that create harm or loss of goodwill to the Visa system

  - – Include all of the following:

    - ▪ Prohibition against the Merchant depositing a Transaction that it knows or should have known to be either fraudulent or not authorized by the Cardholder

    - ▪ Statement that the Merchant is responsible for its employees' actions

    - ▪ Transaction Deposit restrictions

    - ▪ Transaction processing prohibitions

    - ▪ Prohibition against a Merchant depositing a Transaction that does not result from an act between the Cardholder and the Merchant or the Cardholder and a Sponsored Merchant (laundering)

    - ▪ Disclosure of account or Visa Transaction Information prohibitions

    - ▪ A requirement that the Merchant and its Agents comply with the provisions of the Account Information Security Program

- ▪ Merchant responsibility for demonstrating compliance by its Agents with the requirements of the Account Information Security Program

- ▪ A requirement that the Merchant, if undergoing a forensic investigation at the time the Merchant Agreement is signed, fully cooperate with the investigation until completed

- – Remain on file at the Acquirer's place of business

- – Not be assigned or transferred to another Member without the agreement of the Acquirer

- – If used by an Agent, be reviewed by the Acquirer

ID# 0028044	Edition: Apr 2020 | Last Updated: Apr 2020

5.2.1.8   Merchant Agreement Disclosure Requirements and Cancellation Rights – Canada Region

Effective through 31 January 2020 In the Canada Region: Where an Acquirer uses one or more service providers and where a Merchant is required to enter into more than one agreement with the Acquirer and such service provider(s) in connection with its payment acceptance services:

- The Acquirer must provide written disclosure of the following information in a consolidated fashion, before entering into a Merchant Agreement:

  - – The name, coordinates, and contact information of each service provider and the nature of the services being provided by each

  - – The effective date of each agreement

  - – Information on the expiration and renewal for each agreement

  - – Detailed information on any applicable fees and rates for each service provider

  - – Information on how statements will be provided to Merchants

  - – The cancellation terms of each service provider's agreement, including specific information on any cancellation fees that could apply

  - – If point-of-sale services are offered to a Merchant, general information on buying, leasing, or renting options of point-of-sale hardware

  - – The complaint-handling process for each service provider, including how a Merchant can contact the complaints department of each

- The Acquirer must ensure that the Merchant is provided with a copy of the agreed-upon terms for each agreement.

- Except where a Merchant, on its own initiative, enters into separate agreements with unrelated service provider or service providers which are unrelated to the Acquirer, a Merchant must be permitted to cancel all related agreements without penalty, following notification of any new or

increased fees by the Acquirer and/or service provider, in accordance with the *Code of Conduct for the Credit and Debit Industry.*

ID# 0027722	Edition: Apr 2020 | Last Updated: Apr 2020

5.2.1.9   Provision of Merchant Invoices – Europe Region

In the Europe Region: An Acquirer must provide an invoice to its Merchant for MIFs showing all of the following for the invoice period:

- The total number of Transactions processed by the Merchant
- The total value of Transactions processed by the Merchant
- The MIFs assessed to the Merchant which, unless the Merchant has chosen blended pricing, must be broken down by the following Card types:
  - Credit Card and Deferred Debit Card
  - Direct (Immediate) Debit Card
  - Visa Electron Card
  - Visa Commercial Card

ID# 0029650	Edition: Apr 2020 | Last Updated: Oct 2016

5.2.1.10   Communication of Interchange Reimbursement Fee (IRF) Rates – Europe Region

In the Europe Region: An Acquirer must inform its Merchant of the availability of Interchange Reimbursement Fee rates, including for intra-European Economic Area (EEA) Transactions and Domestic Transactions within the EEA.

ID# 0029651	Edition: Apr 2020 | Last Updated: Oct 2016

5.2.1.11   Merchant Category Code (MCC) Assignment

An Acquirer must assign to a Merchant Outlet the MCC that most accurately describes its business.

An Acquirer must assign 2 or more MCCs to a Merchant Outlet if either:

- The Merchant Outlet has deployed an Automated Fuel Dispenser and sells fuel or other goods or services in a Face-to-Face Environment.
- Separate lines of business are located at the same Merchant Outlet and one or more of the following applies:

- A separate Merchant Agreement exists for each line of business.

- Multiple Merchant Outlets on the same premises display different Merchant names.

- One of the lines of business is designated by Visa to be a High-Brand Risk Merchant.

- An Electronic Commerce Merchant Outlet contains a link to a separate electronic commerce website, and each website qualifies for a different MCC.

ID# 0003133	Edition: Apr 2020 | Last Updated: Oct 2015

5.2.1.12   Merchant Name Assignment

The name used to identify a Merchant must be all of the following:

- The name it primarily uses to identify itself to its customers

- Displayed at each Merchant Outlet or on an Electronic Commerce Merchant's website[1] and/or application

- Used consistently, including spelling, in every place that it is used, including, but not limited to, the:

  - Transaction Receipt provided to the Cardholder

  - Authorization Request

  - Clearing Record[2]

  - Dispute, Dispute Response, and Acquirer-initiated pre-Arbitration records

The Acquirer must correct non-compliant Merchant names or those causing Cardholder confusion.

[1] For Electronic Commerce Transactions, the website address may be used, unless the website address is not directly related to the Merchant name.

[2] The Merchant name in the Clearing Record may differ from the Merchant name on the Transaction Receipt if abbreviations are required or supplementary data is used.

ID# 0027816	Edition: Apr 2020 | Last Updated: Apr 2018

5.2.1.13   Acquirer Processing of Visa Debit Category Transactions – Canada Region

In the Canada Region: An Acquirer must be able to process Visa Debit Category Transactions from any Merchant with which the Acquirer has a Merchant Agreement.

ID# 0008078	Edition: Apr 2020 | Last Updated: Oct 2014

5.2.2 Acquirer and Payment Facilitator Responsibilities Related to Deposit Accounts

5.2.2.1 Domiciled Institutions Requirements – LAC Region (Brazil)

In the LAC Region (Brazil): An Acquirer and a Payment Facilitator must both:

- Allow the Merchant and the Sponsored Merchant to choose their Domiciled Institution
- Ensure that the Domiciled Institution chosen by the Merchant and the Sponsored Merchant has a direct contract with Visa

ID# 0029507	Edition: Apr 2020	Last Updated: Apr 2017

5.3 Payment Facilitator, Staged Digital Wallet Operator, and Marketplace Responsibilities and Requirements

5.3.1 Acquirer Responsibilities and Liabilities in Payment Facilitator and Staged Digital Wallet Operator Agreements

5.3.1.1 Required Content of Payment Facilitator Agreement or Staged Digital Wallet Agreement

The Acquirer must include all of the following in a Payment Facilitator Agreement or a Staged Digital Wallet Operator (SDWO) agreement:

- A requirement that the Payment Facilitator and its Sponsored Merchants, or the SDWO comply with the Visa Rules
- A requirement that the Payment Facilitator enter into a contract with each Sponsored Merchant
- The Acquirer's right to immediately terminate a Sponsored Merchant, the Payment Facilitator, an SDWO, or a retailer signed by an SDWO for good cause or fraudulent or other activity or upon Visa request
- Statements specifying that the Payment Facilitator or the SDWO:
  - Is liable for all acts, omissions, Cardholder disputes, and other Cardholder customer service-related issues caused by the Payment Facilitator's Sponsored Merchants, or the retailer signed by an SDWO
  - Is responsible and financially liable for each Transaction processed on behalf of the Sponsored Merchant, or for any disputed Transaction or credit

– Must not transfer or attempt to transfer its financial liability by asking or requiring Cardholders to waive their dispute rights

– Must not permit a Sponsored Merchant to transfer or attempt to transfer its financial liability by asking or requiring Cardholders to waive their dispute rights

– Must not deposit Transactions on behalf of another Payment Facilitator

– Must not contract with a Sponsored Merchant, or a retailer in the case of an SDWO, whose contract to accept Transactions was terminated at the direction of Visa or a government agency

– Must not deposit Transactions from Sponsored Merchants, or retailers signed by an SDWO outside the Acquirer's jurisdiction

– Must provide the names of principals and their country of domicile for each of its Sponsored Merchants, or retailers signed by an SDWO, and Transaction reports to its Acquirer and to Visa upon request

– Must ensure that its Sponsored Merchants comply with the *Payment Card Industry Data Security Standard (PCI DSS)* and the *Payment Application Data Security Standard (PA-DSS)*

ID# 0026431	**Edition: Apr 2020	Last Updated: Oct 2017**

5.3.1.2   Acquirer Liability for Payment Facilitators and Sponsored Merchants

A Sponsored Merchant will be treated as a Merchant of its Payment Facilitator's Acquirer.

An Acquirer that contracts with a Payment Facilitator is liable for all acts, omissions, and other adverse conditions caused by the Payment Facilitator and its Sponsored Merchants, including, but not limited to:

- Related legal costs
- Settlement to the Payment Facilitator or Sponsored Merchant

The acts and omissions caused by a Sponsored Merchant will be treated as those of the Payment Facilitator and those caused by a Payment Facilitator or a Sponsored Merchant as those of the Acquirer.

ID# 0006574	**Edition: Apr 2020	Last Updated: Oct 2017**

5.3.1.3   Acquirer Requirements for Contracting with Payment Facilitators

If an Acquirer contracts with a Payment Facilitator, it must comply with all of the following:

- Be in good standing in all Visa risk management programs

- Be financially sound (as determined by Visa)

- Meet a minimum equity requirement

- Ensure that its registration of its Payment Facilitator, including the attestation of due diligence review, is confirmed by Visa before submitting Transactions on behalf of the Payment Facilitator or its Sponsored Merchant. If the Payment Facilitator is considered to be high-brand risk, it must be registered as a High-Risk Internet Payment Facilitator even if that Payment Facilitator has previously been registered with Visa.

- All of the following:

  - Obtain from Visa a unique Payment Facilitator identifier[1] that must be assigned by the Acquirer to each Payment Facilitator to use in Transaction processing

  - Ensure the Payment Facilitator determines and assigns a unique identifier[1] to each Sponsored Merchant

  - Ensure that every Transaction contains the Payment Facilitator identifier[1] and the Sponsored Merchant identifier, as follows:

    - In an Authorization record, both the Payment Facilitator identifier and the Sponsored Merchant identifier

    - In a Clearing Record, only the Payment Facilitator identifier

- If the Payment Facilitator's annual Visa volume in the Acquirer's jurisdiction exceeds USD 50 million, either:

  - Meet a minimum equity requirement

  - Enter into a direct Merchant Agreement with, and fund, each of the Payment Facilitator's Sponsored Merchants[2]

- Enter into a direct Merchant Agreement with a Sponsored Merchant that exceeds USD 100,000[3] in annual Transaction volume, as follows:[2]

  - For Sponsored Merchants new to the Payment Facilitator, before processing any Transactions

  - For Sponsored Merchants with existing contracts with the Payment Facilitator, the earlier of either:

    - The renewal of the Sponsored Merchant agreement with the Payment Facilitator

    - 2 years after annual Visa volume exceeds USD 100,000[3]

  The Payment Facilitator may continue to provide payment services (including settlement) to the Merchant.

- If the Acquirer settles the proceeds of Transactions submitted by the Payment Facilitator on behalf of its Sponsored Merchants, pay the proceeds into a bank account in the Payment Facilitator location

- Not allow its Payment Facilitator to provide payment services to the following merchant types:[2,4]

  – Internet pharmacies

  – Internet pharmacy referral sites

  – Outbound telemarketers

- Upon Visa request, submit to Visa activity reporting on its Payment Facilitator's Sponsored Merchants that includes all of the following for each Sponsored Merchant:

  – Sponsored Merchant name as it appears in the Merchant name field

  – Sponsored Merchant DBA name

  – Payment Facilitator name

  – Monthly Transaction count and amount

  – Monthly Dispute count and amount

- Ensure that its Sponsored Merchants and the Sponsored Merchants of its Payment Facilitators follow all Merchant-related rules

- Ensure that its Payment Facilitators provide customer service directly or through its Sponsored Merchants

- Ensure that its Payment Facilitators have access to the results of any positive matches on the Visa Merchant Screening Service (VMSS)

- In addition, all of the following:

  – Include in its contract with the Payment Facilitator a clear statement of both the jurisdiction within which the Payment Facilitator may contract with Sponsored Merchants and the category (or categories) of Sponsored Merchants with which it may contract

  – When a Cardholder can access a Payment Facilitator's website and/or application directly, ensure that its Payment Facilitator both:

    ▪ Provides customer service and after-sales support, either directly or via its Sponsored Merchants, in all languages in which services are offered

    ▪ Clearly display customer service contact information or trading office contact information on its website and/or application

  – Ensure that its Payment Facilitator reports Sponsored Merchant and Transaction Information to the Acquirer and, upon request, to Visa

– Ensure that its Payment Facilitator uses the appropriate MCC or other required indicators to identify Merchant or Transaction type

[1] In the LAC Region (Brazil): An Acquirer must send the tax identification and Merchant legal name if it has obtained the Payment Facilitator's consent to do so. If not, the Acquirer must send the Payment Facilitator identifier and the Sponsored Merchant identifier.

[2] In the LAC Region (Brazil): This does not apply.

[3] **Effective through 18 October 2019** In the AP Region (Australia, Hong Kong, India, New Zealand), Canada Region, Europe Region, US Region: USD 1 million
Effective 19 October 2019 In the AP Region (Australia, Hong Kong, India, New Zealand, Taiwan), Canada Region, Europe Region, US Region: USD 1 million

[4] In the Europe Region: This does not apply.

ID# 0026435	Edition: Apr 2020 | Last Updated: Apr 2020

5.3.2   Payment Facilitator, Staged Digital Wallet Operator, and Marketplace Responsibilities and Requirements

5.3.2.1   Assignment of Payment Facilitator, Staged Digital Wallet Operator, or Marketplace Location

An Acquirer must assign the correct location of its Payment Facilitator as the country of the Payment Facilitator's Principal Place of Business.

An Acquirer may assign an additional Payment Facilitator location if all of the following occur in each country:[1,2]

- The Payment Facilitator has a permanent location at which the Payment Facilitator's employees or agents conduct the business activity directly related to the provision of the Payment Facilitator's services to the Sponsored Merchant.

- Cardholder correspondence and judicial process are sent by/delivered to the Payment Facilitator.

- The Payment Facilitator assesses taxes on its provision of Card acceptance services to Sponsored Merchants.

- The Payment Facilitator is subject to local laws and regulations.

- In addition, in the Europe Region: The Payment Facilitator has a business license to operate in the country.

An Acquirer must assign the correct location of a Staged Digital Wallet Operator (SDWO) as the country of the SDWO's Principal Place of Business.

An Acquirer may assign an additional SDWO location[1,2] if all of the following occur in each country:

- The SDWO has a permanent location at which it manages the activities associated with the Staged Digital Wallet.

- The SDWO pays taxes related to revenue earned from the provision of the wallet services to Cardholders and acceptance services to retailers signed by the SDWO, if the country levies such taxes.

- The SDWO is subject to local laws and regulations.

- In the Europe Region: The SDWO has appropriate approvals in place to do business in the country where its retailers receive payments from the SDWO, as required by applicable laws or regulations.

An Acquirer must assign the correct location of its Marketplace as the country of the Marketplace's Principal Place of Business.

An Acquirer may assign additional Marketplace locations if the Transaction is one of the following:

Table 5-1: Allowed Additional Marketplace Locations

Transaction	Additional Marketplace location may be:
Airline, Cruise Line, passenger railway, or other travel	The country from which the first leg of the purchased travel originates
Taxi or ride service	The country in which the journey originates
All other	The country where all of the following occur:[2] • The Marketplace has a permanent location at which its employees or agents conduct the business activity and operations directly related to providing Marketplace services to retailers and Cardholders. • The Marketplace pays applicable taxes. • The address for correspondence and judicial process is in that country.

Visa reserves the right to determine the location of a Marketplace.

[1] The Payment Facilitator or SDWO must contract with an Acquirer in each country and sign applicable Merchant Agreements with Sponsored Merchants or retailers, as applicable.

[2] An exception applies to Payment Facilitator and SDWO locations within the Europe Region, and to Marketplace locations within the European Economic Area, as specified in the *Visa Merchant Data Standards Manual*.

ID# 0029139   Edition: Apr 2020 | Last Updated: Oct 2018

5.3.2.2   Qualification as a Marketplace, Merchant, Payment Facilitator, or Staged Digital Wallet Operator

An entity that deposits a Transaction, receives settlement from, or contracts with an Acquirer is classified as a Merchant if all of the following apply:

- The entity represents itself as selling the goods or services to the Cardholder.

- The entity uses its name primarily to identify its Merchant Outlet to the Cardholder.

- The entity provides recourse to the Cardholder in the event of a dispute.

Otherwise, the entity is classified as one of the following:

- A Staged Digital Wallet Operator (SDWO), if it meets the SDWO criteria

- A Marketplace, if it meets the Marketplace criteria

- A Payment Facilitator

Visa reserves the right to determine whether an entity is a Payment Facilitator, a Marketplace, a Merchant, or an SDWO and may use additional criteria including, but not limited to, the entity's name that appears on the Transaction Receipt and the entity that:

- Owns or takes possession of the goods or services

- Books the sale as revenue

- Provides customer service and handles returns

ID# 0030076   **Edition: Apr 2020 | Last Updated: Oct 2019**

5.3.3   Acquirer Responsibility for Staged Digital Wallet Operators

5.3.3.1   Staged Digital Wallet Operator Requirements

An Acquirer that contracts with a Staged Digital Wallet Operator (SDWO) must comply with all of the following:

- Be in good standing in all Visa risk management programs

- Meet a minimum equity requirement of USD 100 million (USD 500 million if the SDWO's annual Transaction volume exceeds USD 50 million)[1]

- Register the SDWO as a Third Party Agent with Visa

- If the wallet can be used at a retailer that Visa classifies as a High-Brand Risk Merchant, do both of the following before submitting Transactions:

- – Register the SDWO with Visa as a High-Brand Risk Merchant

  – Register with Visa as a High-Brand Risk Merchant any retailer that receives payment from the SDWO

- Obtain a Merchant Verification Value (MVV) for each SDWO

- Process the Transaction as a Card-Absent Environment Transaction

- Use the appropriate business application identifier in all Transaction messages

- Pay the proceeds of Transactions conducted via the SDWO into a bank account in the SDWO location

- Ensure that the SDWO complies with all of the following:

  – At the time of loading the Cardholder information in the Staged Digital Wallet, obtains either written or electronic Cardholder consent to all of the following:

    ▪ Use of the stored account information to initiate Transactions

    ▪ The purpose for which the Cardholder's information will be used

    ▪ The expiration date of the agreement, if applicable

  – Does not assign to a Cardholder a Payment Credential or a credential of a non-Visa general-purpose payment network

  – In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Is located in the same country as the retailer that receives payment from the SDWO.

  – In the Europe Region: The SDWO is either:

    ▪ Located in the same country as the retailer that receives payment from the SDWO

    ▪ Located in any country in the Europe Region, if the SDWO and the retailer have the necessary approvals to do business in the country where the retailer is located

  – Has an acceptance contract with the retailer and conducts appropriate due diligence

  – Does not contract with a Payment Facilitator or another SDWO to process Transactions

  – Displays on the payment screen and all screens that show Account information both:

    ▪ The last 4 digits of the Payment Credential

    ▪ The Visa Brand Mark or the name "Visa" in text immediately next to a Visa payment option

- Ensure that all Transactions using a Staged Digital Wallet comply with *Table 5-2, Staged Digital Wallet Transaction Processing Requirements*

Table 5-2: Staged Digital Wallet Transaction Processing Requirements

Use[2]	MCC	Transaction Indicator	Merchant Outlet Location	Merchant Name
Funding the wallet before the Cardholder makes the purchase[3]	Any of the following: • For account funding, MCC 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [not Money Transfer], Travelers Cheques, and Debt Repayment) • If the funds will be used for a High-Brand Risk Transaction, the applicable High-Brand Risk MCC • If the funds are used for a gambling Transaction, the applicable gambling MCC	• MVV • Business application indicator of WT • AFT Indicator • Appropriate Card-Absent Environment indicator or Electronic Commerce Indicator	The country where the SDWO is located	Name of DWO
Purchase with back-to-back funding, where the funding Transaction is initiated by the SDWO and corresponds to, or is otherwise directly connected to, a specific purchase. An Acquirer must comply with these processing requirements whether the Transaction represents the whole or only a part of the Transaction.[3]	MCC that describes the primary business of the retailer	• MVV • Business application indicator of WT • Appropriate Card-Absent Environment indicator or Electronic Commerce Indicator	The country where the retailer is located	Name of DWO *name of retailer

[1] Visa may waive this requirement in exchange for assurance and evidence of the imposition of risk controls and requirements satisfactory to Visa. Such controls and requirements may include, but are not limited to, the pledging of

additional collateral.

[2] Visa retains the right to determine permitted Transaction types.

[3] If there is a mixed source of funding, for example: when a Cardholder uses a wallet that is partially funded before the Cardholder makes the purchase and partially funded as a back-to-back purchase, each portion must adhere to the rules for the respective Transaction type.

ID# 0029535	Edition: Apr 2020 | Last Updated: Apr 2020

5.3.4   Acquirer Responsibility for Marketplaces

5.3.4.1   Marketplace Qualification Requirements

Visa classifies an entity that meets all of the following as a Marketplace:

- Brings together Cardholders and retailers on an electronic commerce website or mobile application
- Its name or brand is:
  - Displayed prominently on the website or mobile application
  - Displayed more prominently than the name and brands of retailers using the Marketplace
  - Part of the mobile application name or URL
- Handles payments for sales and refunds on behalf of the retailers that sell goods and services through the Marketplace, and receive settlement for Transactions on their behalf
- Is financially liable for Disputes and resolves disputes between Cardholders and retailers by providing either:
  - A decision that binds both Cardholder and retailer
  - A money-back guarantee funded by the Marketplace
- Ensures that no retailer exceeds both:
  - USD 10 million in annual Visa volume through the Marketplace
  - 10% of the Marketplace's annual Visa volume

The following Merchant types are not eligible to be Marketplaces or retailers using a Marketplace:

- Franchises
- Travel agents
- High-Brand Risk Merchants

ID# 0030069	Edition: Apr 2020 | Last Updated: Oct 2019

5.3.4.2   Required Additional Content of Marketplace Agreement

In addition to the required content of a Merchant Agreement, an Acquirer must include all of the following in a Marketplace agreement:

- A requirement that the Marketplace and its retailers comply with the Visa Rules

- A requirement that the Marketplace enter into a contract with each retailer before it deposits Transactions on the retailer's behalf

- The Acquirer's right to prohibit individual retailers from participating in the Visa system and to immediately stop depositing Transactions for any individual retailer for good cause or upon Visa request

- Statements specifying that the Marketplace:

  – Is permitted to process Transactions for retailers located in a different country to the Marketplace, and must ensure that Transactions are legal in the country of the Marketplace and of the retailer

  – Is liable for all acts, omissions, Cardholder disputes, and other Cardholder customer service-related issues caused by the Marketplace's retailers

  – Is responsible and financially liable for each Transaction processed on behalf of a retailer

  – Must not transfer or attempt to transfer, or permit the retailer to transfer or attempt to transfer, its financial liability by asking or requiring Cardholders to waive their dispute rights

  – Must deposit Transactions only on behalf of retailers of goods and services that use the Marketplace's website or application

  – Must not knowingly contract with a retailer whose contract to accept Transactions was terminated at the direction of Visa or a government agency

ID# 0030070	Edition: Apr 2020 | Last Updated: Apr 2018

5.3.4.3   Acquirer Liability for Marketplaces

An Acquirer that contracts with a Marketplace is liable for all acts, omissions, and other adverse conditions caused by the Marketplace and its retailers, including, but not limited to:

- Related legal costs

- Settlement to the Marketplace or retailer

The acts and omissions of a retailer will be treated as those of the Marketplace, and the Acquirer is fully liable for any losses to Visa, its Members, or other stakeholders caused by a Marketplace or its retailers.

ID# 0030071	Edition: Apr 2020 | Last Updated: Apr 2018

5.3.4.4   Marketplace Acquirer Requirements

An Acquirer that contracts with a Marketplace must comply with all of the following:

- Be in good standing in all Visa risk management programs

- Meet a minimum equity requirement of USD 100 million (USD 500 million if the Marketplace's annual Visa volume exceeds USD 50 million)[1]

- Register the Marketplace as a Third Party Agent with Visa

- Obtain written confirmation from Visa that the entity qualifies as a Marketplace

- Ensure that adequate due diligence is applied to retailers using a Marketplace and that risk management controls are in place to do all of the following:

    - Prevent Transactions that are illegal in the location of the Marketplace, the location of its retailers, or the location of the Cardholder

    - Prevent the sale of counterfeit products or goods that infringe intellectual property

    - Provide a process to investigate and remediate rights-holder complaints

    - Ensure that the Marketplace and its retailers are not engaged in any activity that could cause harm to the Visa brand

    - Ensure compliance with all laws, regulations, requirements, and Visa Rules relating to anti-money laundering and anti-terrorist funding

- Ensure that the Marketplace complies with all Visa Rules relating to Merchants unless otherwise stated or unless the rule is inconsistent with a rule specific to Marketplaces

- Obtain from Visa a unique Marketplace identifier and include the Marketplace identifier in all Transaction messages[2]

[1] Visa may waive this requirement in exchange for assurance and evidence of the imposition of risk controls and requirements satisfactory to Visa. Such controls and requirements may include, but are not limited to, the pledging of additional collateral.

[2] In the LAC Region (Brazil): An Acquirer must send the tax identification and Merchant legal name if it has obtained the Marketplace's consent to do so. If not, the Acquirer must send the Marketplace identifier and the retailer identifier.

ID# 0030072	Edition: Apr 2020 | Last Updated: Oct 2019

5.3.4.5   Reporting Requirements for Acquirers of Marketplaces

An Acquirer that contracts with a Marketplace must recertify annually that information provided to obtain written approval from Visa remains materially unchanged, and inform Visa immediately if

there is a material change in the information provided to obtain approval from Visa to treat the entity as a Marketplace. Visa approval is withdrawn if the Acquirer fails to comply with this requirement.

An Acquirer must, for an international Marketplace or upon Visa request, within 90 days of registration and each quarter thereafter, report to Visa all of the following:

- Total Marketplace Transaction value

- Total Marketplace Transaction value generated by retailers in the same country as the Marketplace[1,2]

- Total domestic Marketplace Transaction value generated by retailers in a different country to the Marketplace ("International Retailer Volume")[3]

- Total international Marketplace Transaction value

[1] Marketplace volume where the Marketplace, Issuer, and retailer are all in the same country.

[2] In the Europe Region: For a Marketplace located within the European Economic Area (EEA), this includes Transactions where the Marketplace's retailers are also located within the EEA.

[3] Marketplace volume where the Marketplace and Issuer are in the same country, and the retailer is in a different country.

ID# 0030073	Edition: Apr 2020 | Last Updated: Oct 2019

5.4   Merchant and Cardholder Interaction

5.4.1   Honoring Cards

5.4.1.1   Acceptance of Visa Cards Issued by Non-Canada Issuers – Canada Region

In the Canada Region: A Merchant that accepts Visa Cards must accept any valid Visa Card issued by a non-Canada Issuer, as specified in the Visa Rules.

ID# 0008384	Edition: Apr 2020 | Last Updated: Oct 2014

5.4.2   Conditions of Card Acceptance and Cardholder Rights

5.4.2.1   Visa Contactless Transaction Requirement in Australia – AP Region

A Merchant or an Acquirer must not override a Cardholder's choice to access the credit account on a Credit Card with multiple contactless Payment Applications used at a Contactless Acceptance Device.

ID# 0028916   Edition: Apr 2020 | Last Updated: Apr 2020

5.4.2.2   Maximum Transaction Amount – US Region and US Territories

In the US Region or a US Territory, a Merchant must not establish a maximum Transaction amount as a condition for honoring a Visa Card, except for a Transaction conducted with a Credit Card issued in the US Region or a US Territory.

Only the following Merchants may establish a maximum Transaction amount for the Card type specified above:

- An agency of the US federal government
- A Merchant assigned one of the following MCCs:
  - 8220 (Colleges, Universities, Professional Schools, and Junior Colleges)
  - 8244 (Business and Secretarial Schools)
  - 8249 (Trade and Vocational Schools)

Any maximum Transaction amount imposed must not be discriminatory between Issuers or between Visa and another payment network.

ID# 0026411   Edition: Apr 2020 | Last Updated: Apr 2020

5.4.2.3   Minimum Transaction Amount – US Region and US Territories

In the US Region or a US Territory, a Merchant must not establish a minimum Transaction amount as a condition for honoring a Card, except for a Transaction conducted with a Credit Card issued in the US Region or a US Territory.

The minimum Transaction amount must not be greater than USD 10 and must not be discriminatory between Issuers or between Visa and another payment network.

ID# 0026410   Edition: Apr 2020 | Last Updated: Apr 2020

5.4.2.4   Disclosure to Cardholders of Return, Refund, and Cancellation Policies

If a Merchant restricts the return of goods or cancellation of services, it must clearly disclose to a Cardholder its return, refund, and cancellation policies, as follows:

- For Card-Present Environment Transactions, at the Point-of-Transaction before the Cardholder completes the Transaction. If the disclosure is on the back of the Transaction Receipt or in a separate contract, it must be accompanied by a space for the Cardholder's signature or initials,

which must be completed by the Cardholder as acceptance of the Merchant's policy.

- For Transactions at an Electronic Commerce Merchant, during the sequence of pages before final checkout, and include a "click to accept" button, checkbox, or other acknowledgement. The disclosure may be a link to a separate page if that link forms part of the "click to accept" acknowledgement and refers to the return, refund, or cancellation policy.

- For Card-Absent Environment Transactions that are not Electronic Commerce Transactions, through mail, email, or text message

- In addition, for a Guaranteed Reservation, the Merchant must:

  - Disclose the date and time the stay or rental will begin and the location where the accommodation, merchandise, or services will be provided

  - Agree to hold the reservation unless it is cancelled according to the agreed policy. That policy must include, but is not limited to the following:

    • Date and time by which the Cardholder must cancel the reservation to avoid a penalty

    • Amount the Cardholder must pay if the reservation is not properly cancelled by the deadline and the Cardholder does not claim the accommodations, merchandise, or services within 24 hours of the agreed time

  - If unable to honor the reservation, provide the agreed accommodations, merchandise, or services, or comparable accommodations, merchandise, or services, at no additional cost to the Cardholder or as agreed by the Cardholder

A Merchant must not require a Cardholder to waive the right to dispute a Transaction with the Issuer.

ID# 0008771	Edition: Apr 2020 | Last Updated: Apr 2018

5.4.3 Merchant Use of Cardholder Account Information

5.4.3.1 Merchant Use of Payment Credential, Cardholder Signature, Card Verification Value 2 (CVV2), or Stored Credential

A Merchant must comply with all of the following:

- Not request or use a Payment Credential for any purpose that is not related to payment for goods and services, except as specified in *Section 5.4.3.2, Use of a Payment Credential for Service Access*.

- Store and reproduce the signature only for the Transaction for which the signature was obtained

- Reproduce the signature only upon specific written request from the Acquirer or in response to a valid Retrieval Request

- Use a Stored Credential only as agreed with the Cardholder

- Not require a Cardholder to complete a postcard, or similar device, that will cause the Card account data or the Cardholder's signature to be in plain view when mailed

- Not request a Card Verification Value 2 (CVV2) from the Cardholder on any written form

- Not request a Card Verification Value 2 (CVV2) from the Cardholder for a Card-Present Environment Transaction

- Display on the payment screen and all screens that show account information both:

  – The last 4 digits of the Payment Credential

  – The Visa Brand Mark or the name "Visa" in text immediately next to a Visa payment option

ID# 0008585   Edition: Apr 2020 | Last Updated: Apr 2020

5.4.3.2   Use of a Payment Credential for Service Access

A Merchant may use a Payment Credential for the purpose of providing access to a service only if either:

- The service was purchased using that Payment Credential.

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: The Card is a Prepaid Card and the service was purchased with cash at a Merchant assigned one of the following MCCs:

  – 4111 (Local and Suburban Commuter Passenger Transportation, Including Ferries)

  – 4112 (Passenger Railways)

  – 4131 (Bus Lines)

A Merchant's use of a Payment Credential to provide access to a service must be limited to the generation of a secure, irreversible, and unique access token both:

- At the time the service is purchased

- At the point of access to verify the access token

At the time of purchase, the Merchant must disclose to the Cardholder any restrictions, additional conditions, or customer service policies that may be relevant to the Cardholder's ability to access the service purchased.

ID# 0027232   Edition: Apr 2020 | Last Updated: Apr 2020

5.4.3.3   Access Token Restrictions

A Merchant that uses Visa account information to generate an access token must not:

● Require a Cardholder to perform any Cardholder Verification or present identification in order to accept the Visa account information as a means to access the service

● Use the Visa account information, instead of an access token, to verify eligibility at the point of access

● Transmit Visa account information except as required for processing an associated Visa Transaction

● Store the Visa account information at the point of access

● Use Visa-Owned Marks at the point of access, unless the point of access is also a Point-of-Transaction

● Use or store Visa account information for any purpose other than to generate an Access Token

ID# 0027233	Edition: Apr 2020 | Last Updated: Apr 2018

5.4.3.4   Reusing Redemption Credentials – Europe Region

In the Europe Region: If a Payment Credential is used to access previously purchased goods and/or services more than once using the same redemption credentials each time, the Merchant must:

● Permit the transfer of a Payment Credential's purchase record to another Payment Credential for a legitimate reason (for example: the Card was lost or stolen)

● Submit an Account Verification of the Card to which the purchase record is being transferred, whenever a Card's purchase record is transferred to another Card

ID# 0029682	Edition: Apr 2020 | Last Updated: Apr 2020

5.5   Merchant Verification of Card and Cardholder

5.5.1   Card and Cardholder Validation

5.5.1.1   Card and Cardholder Validation in a Face-to-Face Environment

An Acquirer or a Merchant must validate a Card and Cardholder in a Face-to-Face Environment, as follows:

Table 5-3: Card and Cardholder Validation in a Face-to-Face Environment

Description	Manual Cash Disbursements and Quasi-Cash Transactions	All Other Face-to-Face Transactions
Validate the identity of the Cardholder by reviewing the Cardholder's identification document (for example: a valid passport, valid driver's license with photo, other government-issued identification, Visa Card containing the Cardholder's photograph). Describe the identification on the Transaction Receipt, excluding the document number or any other identifying information. These requirements do not apply to PIN- or Consumer Device Cardholder Verification Method (CDCVM)-authenticated Manual Cash Disbursements or Quasi-Cash Transactions if the Transaction amount is either: • For a Chip Transaction, USD 500 or less (or local currency equivalent) • For a US Domestic Transaction, any amount	X[1]	

Verify the Cardholder using one of the following:[2]
 	
• For a Transaction at a Compliant Chip Reading Device, act on the Cardholder Verification Method (CVM) list on the Card or Contactless Payment Device. A Merchant may process a Transaction without a Cardholder signature.
 	
• For a Transaction that takes place at a Magnetic-Stripe-only Acceptance Device, either:
 	
  – Signature[3]
 	
  – PIN
 	
The requirement to verify the Cardholder does not apply to Visa Easy Payment Service (VEPS) Transactions.
	X	X

[1] In the Europe Region (United Kingdom): The validation of a Cardholder's identity using secondary identification is not required for the purchase of gaming chips in casinos.

[2] **Effective through 17 April 2020** In the AP Region (Japan, Philippines) or where applicable laws or regulations require a Cardholder Verification Method to be captured, a Merchant must verify the Cardholder using PIN, CDCVM, or a signature. This does not apply to either Visa Easy Payment Service (VEPS) Transactions or Transactions that take place with a Card that does not contain a signature panel.

Table 5-3: Card and Cardholder Validation in a Face-to-Face Environment (continued)

Description	Manual Cash Disbursements and Quasi-Cash Transactions	All Other Face-to-Face Transactions
Effective 18 April 2020 Where applicable laws or regulations require a Cardholder verification Method to be captured, a Merchant must verify the Cardholder using PIN, CDCVM or a signature.		
[3] For a Transaction that takes place with a Card that does not contain a signature panel, the Merchant must capture a signature but is not required to verify it.		

ID# 0008769	Edition: Apr 2020 | Last Updated: Apr 2020

5.6   Surcharges, Convenience Fees, and Service Fees

5.6.1   Surcharges – Allowances, Requirements, Restrictions, Amounts, and Disclosures

5.6.1.1   Surcharges – AP Region (Australia)

In the AP Region (Australia): If a Merchant adds a Surcharge to a Transaction, the Surcharge amount must comply with all of the following:

- Be limited to the "reasonable costs of acceptance" of a Visa Card (or Visa Cards) as that concept is defined by the Reserve Bank of Australia and by applicable laws or regulations

- Not include the cost of accepting any non-Visa payment card

- Be clearly disclosed to the Cardholder before the completion of the Transaction. The Cardholder must be given the opportunity to cancel without penalty after the Surcharge is disclosed.

- Be charged only by the Merchant that provides the goods or services to the Cardholder. The Merchant must not permit a third party to charge a Cardholder a separate or additional amount in respect of the cost of acceptance of the Visa Card, but the Merchant may include third-party costs relevant to accepting a Visa Card as part of its Surcharge.

- Not differ according to Issuer

- Be different for Credit Card Transactions and Debit Card Transactions if the "reasonable cost of acceptance" varies between the 2 Transactions

- Be assessed only on the final total amount charged for the goods or services, after any discount or rebate from the Merchant has been applied

- Be added to the Transaction amount and not collected separately[1]

[1] A government Merchant may collect the Surcharge amount separately and may use a third party to deposit Transactions if it is assigned one of the following MCCs:

  - 9211 (Court Costs, Including Alimony and Child Support)

  - 9222 (Fines)

  - 9223 (Bail and Bond Payments)

  - 9311 (Tax Payments)

  - 9399 (Government Services [Not Elsewhere Classified])

  - 9405 (Intra-Government Purchases)

ID# 0027589	Edition: Apr 2020	Last Updated: Apr 2020

5.6.1.2   Surcharge Disclosure Requirements – AP Region (Australia)

In the AP Region (Australia): A Merchant that assesses a Surcharge must do all of the following:

- Inform the Cardholder that a Surcharge is assessed

- Inform the Cardholder of the Surcharge amount or rate

- Not describe the Surcharge as, or inform the Cardholder that the Surcharge is, assessed by Visa or a financial institution

- Include notices, signs, or decals disclosing that the Merchant assesses a Surcharge. Such notices, signs, or decals must be in a conspicuous location or locations at the Merchant's physical point of sale, or, in the absence of a physical point of sale, prominently during an Electronic Commerce Transaction or communicated clearly in a telephone order so as it can be reasonably assured that all Cardholders presenting a Visa Card will be aware of the Surcharge.

- Clearly display or communicate the Surcharge disclosure in the Transaction environment or process, including (if there is a physical point of sale) at the terminal/cashier's desk. The disclosure must be of as high a contrast as any other signs or decals displayed.

A Merchant must clearly and prominently disclose any Surcharge that will be assessed.

The disclosure at the point of sale must include both:

- The exact amount or percentage of the Surcharge

- A statement that the Surcharge is being assessed by the Merchant

For an Electronic Commerce Transaction, a Mail/Phone Order Transaction, and an Unattended Transaction, the Cardholder must be provided the opportunity to cancel the Transaction subsequent to the Surcharge disclosure.

For example, the requirement for clear and prominent disclosure will be satisfied if the disclosure is made consistent with *Table 5-4, Surcharge Disclosure – AP Region (Australia).*

Table 5-4: Surcharge Disclosure – AP Region (Australia)

Transaction Type	Point-of-Entry	Point-of-Sale
Face-to-Face Transaction	N/A	Every Customer check-out or payment location, in a minimum 16-point Arial font
Electronic Commerce Transaction	The first page that references credit card brands accepted, in a minimum 10-point Arial font	Checkout page, in a minimum 10-point Arial font
Mail order Transaction	The first page of the catalog that references credit card brands accepted, in a minimum 8-point Arial font. The disclosure must also provide instructions for calculating the amount of the Surcharge to be applied and added to the total Transaction amount.	Mail order form, in a minimum 8-point Arial font
Telephone order Transaction	The first page of the catalog that references credit card brands accepted, in a minimum 8-point Arial font. The disclosure must also provide instructions for calculating the amount of the Surcharge to be applied and added to the total Transaction amount.	Verbal notice from the telephone order clerk, including Surcharge amount
Unattended Transaction	N/A	On the Unattended Cardholder-Activated Terminal or virtual disclosure on the payment terminal screen, in a minimum 16-point Arial font

Visa Product and Service Rules

5 Acceptance

Visa Core Rules and Visa Product and Service Rules

5.6.1.3   Notification of Intent to Assess Surcharges – US Region and US Territories

In the US Region or a US Territory: An Acquirer must both:

- Ensure that its Merchant notifies Visa and its Acquirer in writing at least 30 calendar days before assessing a US Credit Card Surcharge. Notice to Visa can be provided as specified on the "Merchant Surcharge Notification" link at *www.visa.com*.

- Inform Visa upon request of all notifications of intent to surcharge received from its Merchants.

ID# 0027544   Edition: Apr 2020 | Last Updated: Oct 2014

5.6.1.4   Similar Treatment of Visa Transactions – US Region and US Territories

A Merchant must not assess a US Credit Card Surcharge on Visa Credit Card Transactions in a specific payment channel if either:

- The Merchant is prohibited or effectively prohibited by a Competitive Credit Card Brand from assessing surcharges on the Competitive Credit Card Brand's products in that payment channel.

- The Merchant's ability to surcharge a Competitive Credit Card Brand in that payment channel is limited by that Competitive Credit Card Brand in any manner[1] and the Merchant assesses a US Credit Card Surcharge on conditions that are not the same as the conditions on which the Merchant would be allowed to surcharge transactions of the Competitive Credit Card Brand in that payment channel, or on which the Merchant actually surcharges transactions of the Competitive Credit Card Brand in that payment channel, after accounting for any discounts or rebates offered at the Point-of-Transaction.

This prohibition does not apply and a Merchant may assess a US Credit Card Surcharge on Visa Credit Card Transactions if one of the following:

- The Competitive Credit Card Cost of Acceptance or the Competitive Credit Card Product Cost of Acceptance to the Merchant is less than the Visa Credit Card Cost of Acceptance or Visa Credit Card Product Cost of Acceptance to the Merchant and the Competitive Credit Card Brand does not prohibit or effectively prohibit surcharging credit card transactions.

- The Competitive Credit Card Brand prohibits or effectively prohibits surcharging on credit cards and the Merchant actually surcharges the Competitive Credit Card Brand's transactions in an amount at least equal to the lesser of either:

  – The Competitive Credit Card Cost of Acceptance

  – The amount of the US Credit Card Surcharge imposed on a Visa Credit Card

- There is an agreement between the Merchant and the Competitive Credit Card Brand in which the Merchant waives or in any other way restrains or limits its ability to surcharge transactions on that Competitive Credit Card Brand, provided that:

– The agreement is for a fixed duration, is not subject to an "evergreen clause" (i.e., automatically renewed unless terminated by the parties to the agreement) and is not a standard agreement generally offered by the Competitive Credit Card Brand to multiple merchants.

– The Merchant's acceptance of the Competitive Credit Card Brand as payment for goods or services is unrelated to and not conditional upon the Merchant's entry into such agreement.

– The agreement is supported by the exchange of material value.

– The agreement expressly specifies a price under which the Merchant may accept the Competitive Credit Card Brand's products and surcharge those transactions up to the Merchant's Merchant Discount Rate for the Competitive Credit Card Brand, after accounting for any discounts or rebates offered by the Merchant at the Point-of-Transaction.

[1] This provision does not apply if the Competitive Credit Card Brand prohibits only surcharging for an amount greater than the Competitive Credit Card Cost of Acceptance.

ID# 0027541   **Edition: Apr 2020 | Last Updated: Oct 2014**

5.6.1.5   US Credit Card Surcharge Requirements – US Region and US Territories

In the US Region or a US Territory: A Merchant may assess a fixed or variable US Credit Card Surcharge on a Visa Credit Card Transaction, subject to applicable laws or regulations.

The Merchant may assess a US Credit Card Surcharge by either:

- Applying the same fixed or variable US Credit Card Surcharge to all Visa Credit Card Transactions (brand level)

- Applying the same fixed or variable US Credit Card Surcharge to all Visa Transactions of the same credit product type (product level)

The US Credit Card Surcharge at the brand level must be the same for all Visa Credit Card Transactions, regardless of the Card's Issuer or the product type, and after accounting for any discounts or rebates offered by the Merchant on Visa Credit Card Transactions at the Point-of-Transaction.

The US Credit Card Surcharge at the product level must be the same for Transactions on a particular Visa Credit Card product type, regardless of the Card's Issuer, and after accounting for any discounts or rebates offered by the Merchant on Visa Credit Card Transactions on the product type at the Point-of-Transaction.

A Merchant must not assess a US Credit Card Surcharge on Visa Credit Card Transactions at both the brand and product level.

The US Credit Card Surcharge must be included in the Transaction amount.

ID# 0027539   Edition: Apr 2020 | Last Updated: Oct 2014

5.6.1.6   US Credit Card Surcharge Maximum Amount – US Region and US Territories

In the US Region or a US Territory: A US Credit Card Surcharge assessed at the brand level, as specified in *Section 5.6.1.5, US Credit Card Surcharge Requirements – US Region and US Territories,* must not exceed the Merchant's Visa Surcharge Cap.

In the US Region or a US Territory: A US Credit Card Surcharge assessed at the product level, as specified in *Section 5.6.1.5, US Credit Card Surcharge Requirements – US Region and US Territories,* must not exceed the Merchant's Visa Credit Card Surcharge Cap less the Debit Card Cost of Acceptance.

In no case may the US Credit Card Surcharge amount exceed the Maximum Surcharge Cap.

ID# 0027540   Edition: Apr 2020 | Last Updated: Oct 2014

5.6.1.7   US Credit Card Surcharge Disclosure Requirements – US Region and US Territories

In the US Region or a US Territory: A Merchant must, at both the point of entry into the Merchant Outlet and the Point-of-Transaction, clearly and prominently disclose any US Credit Card Surcharge that will be assessed.

The disclosure at the Point-of-Transaction must include all of the following:

- The exact amount or percentage of the US Credit Card Surcharge

- A statement that the US Credit Card Surcharge is being assessed by the Merchant and is only applicable to credit Transactions

- A statement that the US Credit Card Surcharge amount is not greater than the applicable Merchant Discount Rate for Visa Credit Card Transactions at the Merchant

Merchants with Acceptance Devices that offer Cardholder choice for debit Transactions in the form of "credit" and "debit" buttons must ensure that:

- Debit Card Transactions are not assessed a US Credit Card Surcharge

- It is made clear to the Cardholder that surcharges are not permitted on debit Transactions regardless whether a Cardholder selects the "credit" or "debit" button

For an Electronic Commerce Transaction, a Mail/Phone Order Transaction, and an Unattended Transaction, the Cardholder must be provided the opportunity to cancel the Transaction subsequent to the US Credit Card Surcharge disclosure.

Visa Product and Service Rules

5 Acceptance

Visa Core Rules and Visa Product and Service Rules

For example, the requirement for clear and prominent disclosure will be satisfied if the disclosure is made consistent with *Table 5-5, Surcharge Disclosure – US Region and US Territories*:

Table 5-5: Surcharge Disclosure – US Region and US Territories

Transaction Type	Point-of-Entry	Point-of-Transaction
Face-to-Face Transaction	Main entrance(s) of the Merchant Outlet, in a minimum 32-point Arial font, but in any case no smaller or less prominent than surrounding text	Every customer checkout or payment location, in a minimum 16-point Arial font, but in any case no smaller or less prominent than surrounding text
Electronic Commerce Transaction	The first page that references credit card brands accepted, in a minimum 10-point Arial font, but in any case no smaller or less prominent than surrounding text	Checkout page, in a minimum 10-point Arial font, but in any case no smaller or less prominent than surrounding text
Mail order Transaction	The first page of the catalog that references credit card brands accepted, in a minimum 8-point Arial font, but in any case no smaller or less prominent than surrounding text	Mail order form, in a minimum 10-point Arial font, but in any case no smaller or less prominent than surrounding text
Telephone order Transaction	The first page of the catalog that references credit card brands accepted, in a minimum 8-point Arial font, but in any case no smaller or less prominent than surrounding text	Verbal notice from the telephone order clerk, including US Credit Card Surcharge amount
Unattended Cardholder-Activated Terminal	Main entrance(s) of the Merchant Outlet (if applicable) (for example: gas [petrol] station store) in a minimum 32-point Arial font, but in any case no smaller or less prominent than surrounding text	On the Unattended Cardholder-Activated Terminal or virtual disclosure on the payment terminal screen, in a minimum 16-point Arial font, but in any case no smaller or less prominent than surrounding text

ID# 0027545   Edition: Apr 2020 | Last Updated: Apr 2020

5.6.2 Convenience Fees – Allowances, Requirements, Restrictions, Amounts, and Disclosures

5.6.2.1 Convenience Fees – AP, CEMEA, and US Regions

In the AP Region, CEMEA Region (Russia), US Region: A Merchant that charges a Convenience Fee must ensure that the fee is assessed as follows:

Table 5-6: Convenience Fee Requirements

Convenience Fee Requirement	AP Region	CEMEA Region (Russia)	US Region
Charged for a bona fide convenience in the form of an alternative payment channel outside the Merchant's customary payment channels and not charged solely for the acceptance of a Card	X	X	X
Added only to a Transaction completed in a Card-Absent Environment	X		X
Not charged if the Merchant operates exclusively in a Card-Absent Environment	X		X
Added only to a domestic Unattended Transaction, excluding Transactions at Automated Fuel Dispensers, Telephone Service Transactions, or ATM Cash Disbursements		X	
Charged only by the Merchant that provides goods or services to the Cardholder	X		X
Applicable to all forms of payment accepted in the payment channel	X	X	X
Disclosed clearly to the Cardholder: • As a charge for the alternative payment channel convenience • Before the completion of the Transaction. The Cardholder must be given the opportunity to cancel.	X	X	X
A flat or fixed amount, regardless of the value of the payment due In the AP Region: An ad valorem amount is allowed as required by applicable laws or regulations. In the CEMEA Region (Russia): The amount must not exceed: • RUB 35 for Transactions processed with MCC 4814	X	X	X

Table 5-6: Convenience Fee Requirements (continued)

Convenience Fee Requirement	AP Region	CEMEA Region (Russia)	US Region
• RUB 60 for Transactions processed with MCC 4900 • RUB 48 for all other Transactions			
Included as part of the total amount of the Transaction and not collected separately	X	X	X
Not charged in addition to a surcharge	X	N/A[1]	X
Not charged on a Recurring Transaction or an Installment Transaction	X	X	X
[1] Surcharging is not allowed.			

ID# 0027492   Edition: Apr 2020 | Last Updated: Apr 2020

5.6.2.2   Acceptance Device Disclosure Requirements for Convenience Fees – CEMEA Region (Russia)

In the CEMEA Region (Russia): If a Merchant or third party charges a Convenience Fee, the Acceptance Device must do all of the following:

- Inform the Cardholder that a Convenience Fee will be charged for the alternative payment channel convenience, in addition to other Issuer charges. The disclosure must both:
    - Be as high a contrast or resolution as any other graphics on the Acceptance Device
    - Contain the notice:
      Fee Notice: "(Name) will assess a fee to cardholders for transactions at this terminal. This fee is added to the amount of your transaction and is in addition to any fees that may be charged by your financial institution."
- Disclose to the Cardholder the amount of the Convenience Fee
- Identify the recipient of the Convenience Fee
- Request Cardholder approval of the Convenience Fee
- Provide the ability for the Cardholder to cancel the Transaction without incurring a fee or penalty

ID# 0025573   Edition: Apr 2020 | Last Updated: Oct 2014

5.6.3   Service Fees – Allowances, Requirements, Restrictions, Amounts, and Disclosures

5.6.3.1   Service Fee Assessment Requirements – Canada, CEMEA (Egypt, Russia), LAC (Trinidad and Tobago), and US Regions

A Service Fee may only be charged by a Merchant, Acquirer, or third party in countries specified in *Table 5-7, Service Fee Assessment Permitted MCCs.*

Table 5-7: Service Fee Assessment Permitted MCCs

Allowed MCCs are:	Canada Region	CEMEA Region (Egypt)	CEMEA Region (Russia)	Effective 15 December 2019 LAC Region (Trinidad and Tobago)	US Region
4900 (Utilities – Electric, Gas, Water, Sanitary)	X	X			
6513 (Real Estate Agents and Managers – Rentals)	X				
9311 (Tax Payments)	X	X	X	X	X
9399 (Government Services [Not Elsewhere Classified])		X	X	X	X
9222 (Fines)	X	X	X	X	X
9211 (Court Costs, Including Alimony and Child Support)		X	X	X	X
8220 (Colleges, Universities, Professional Schools, and Junior Colleges)	X	X			X
8299 (Schools and Educational Services [Not Elsewhere Classified])		X			
8211 (Elementary and Secondary	X	X			X

Table 5-7: Service Fee Assessment Permitted MCCs (continued)

Allowed MCCs are:	Canada Region	CEMEA Region (Egypt)	CEMEA Region (Russia)	Effective 15 December 2019 LAC Region (Trinidad and Tobago)	US Region
Schools)					
8244 (Business and Secretarial Schools)		X			X
8249 (Vocational and Trade Schools)		X			X
8241 (Correspondence Schools)		X			
8351 (Child Care Services)	X				
5541 (Service Stations)		X			
5542 (Automated Fuel Dispensers)		X			
9223 (Bail and Bond Payments)		X	X		
9402 (Postal Services – Government Only)		X			
8050 (Nursing and Personal Care Facilities)	X				

A Merchant, third party, or Acquirer that charges a Service Fee must comply with the following requirements, unless otherwise specified in *Table 5-8, Service Fee Assessment Exceptions*.

- Accept Visa as a means of payment in all channels where payments are accepted (for example, in a Face-to-Face Environment and a Card-Absent Environment, as applicable)

- Be authorized to process tax payment Transactions if the Service Fee is charged by a government taxing authority or its third party

- Disclose the fee clearly to the Cardholder as a Service Fee, or local language equivalent, before the Transaction is completed and provide the ability for the Cardholder to cancel the Transaction without incurring a fee or penalty

- Not represent the Service Fee as a fee charged by Visa

- Ensure that the Service Fee amount is:

  - A reasonable reflection of the costs associated with completing the Transaction (such as the Merchant Discount Rate, Merchant service fee, or any other costs paid to third parties for services directly related to accepting a Card) and, where possible, capped

  - A flat, fixed, banded, or ad valorem amount, regardless of the value of the payment due, as required by applicable laws or regulations

  - Assessed only on the final Transaction amount, after all discounts and rebates have been applied during the Transaction

  - Not charged in addition to a surcharge or Convenience Fee

Table 5-8: Service Fee Assessment Exceptions

	Canada Region	**CEMEA Region (Egypt and Russia only)**	**US Region**
These entities may assess Service Fees:	A Merchant in a permitted category, or its third party, that accepts Visa in all Card-Absent Environments where payments are accepted	A government Merchant, and, in Egypt, a fuel Merchant, its Acquirer, or its third party, that complies with the following, as applicable: • Is registered with Visa • In Russia, also includes its assigned Merchant Verification Value in the Authorization Request and Clearing Record	A government agency or education Merchant, or its third party, that complies with all of the following: • Is registered with Visa • Is assigned a unique Merchant Verification Value
The Service Fee amount:	• Must be limited to 1.5% of the final Transaction amount for debit and 2.5% of the final Transaction amount for credit and prepaid • If assessed by a third party, may be processed as a separate Transaction • Must not be greater than	• Must be flat or variable	• If assessed by a Merchant, may be processed as a separate Transaction • If assessed by a third party in a Card-Absent Environment, must be processed as a separate Transaction

Table 5-8: Service Fee Assessment Exceptions (continued)

	Canada Region	CEMEA Region (Egypt and Russia only)	US Region
	the Service Fee charged on a similar Transaction completed with a similar form of payment • Must be the same as any Service Fee charged to any other Issuer's similar card products		

ID# 0029275   Edition: Apr 2020 | Last Updated: Apr 2020

5.7   Acceptance Devices

5.7.1   Acceptance Device Requirements – All Devices

5.7.1.1   Acceptance Device Requirements

An Acceptance Device must comply with the Transaction Acceptance Device Requirements and all of the following requirements applicable to the device:

Table 5-9: Acceptance Device Requirements

Acceptance Device Type	Requirements
All	• Act upon Service Codes or request Online Authorization • Accept all 16-digit Payment Credentials • Display the appropriate acceptance Mark • Use the proper POS Entry Mode code • If not Chip-enabled, be able to process a key-entered Transaction[1] • For an Acceptance Device installed or upgraded on or after 14 October 2017, make available to the Cardholder all Transaction interfaces supported by the Merchant.[2] A Merchant with an Acceptance Device deployed as of 14 October 2017 that does not make all interfaces available may continue to deploy such an Acceptance Device if

Visa Core Rules and Visa Product and Service Rules

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements

	ADVT and, if applicable, CDET testing (or, in the Europe Region, Visa payWave Test Tool [VpTT]) was successfully completed on the hardware and software combination before 14 October 2017.
	
	 • In the AP Region: All of the following:
	
	   – Support contact Chip-initiated Transactions (excluding ATMs)
	
	   – **Effective through 31 March 2023** Accept Contactless Transactions, if deployed at a new Merchant or as an upgrade for an existing Merchant[3]
	
	   – **Effective 1 April 2023** Accept Contactless Transactions[3]
	
	   – In Australia and New Zealand, for devices in a Face-to-Face Environment, activate the PIN pad to enable PIN Transactions
	
	 • In the CEMEA Region: All of the following:
	
	   – Support contact Chip-initiated Transactions
	
	   – **Effective through 31 March 2023** Accept Contactless Transactions, if contactless-capable, deployed at a new Merchant, or deployed as an upgrade for an existing Merchant[3]
	
	   – **Effective 1 April 2023** Accept Contactless Transactions[3]
	
	   – **Effective 18 April 2020** In Russia: For an ATM installed or upgraded on or after 18 April 2020, be contactless-capable.
	
	 • **Effective 17 October 2020** In the Canada Region: Be a Chip-Reading Device, excluding Unattended Cardholder-Activated Terminals
	
	 • In the Europe Region: All of the following:
	
	   – Be a Chip-Reading Device
	
	   – Accept Contactless Transactions[4]
	
	   – In the Europe Region (Czech Republic, Hungary, Poland, Slovakia) Comply with the *Visa Europe Contactless Terminal Requirements and Implementation Guide* Version 1.5 or later
	
	   – Accept all 11-19 digit Payment Credentials that contain a valid BIN
	
	 • In the LAC Region: All of the following:
	
	   – **Effective through 31 March 2023** Accept Contactless Transactions, if deployed at a new Merchant or as an upgrade for an existing Merchant[5]

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements
	– **Effective 1 April 2023** Accept Contactless Transactions[6]
ATM	Comply with all requirements specified in the *Visa Product and Service Rules: ATM*

Contact Chip	• Be EMV-Compliant and approved by EMVCo
	
	• Accept and process VIS and Common Core Definition Chip Cards
	
	• Be able to read a Magnetic Stripe and complete a Magnetic Stripe-read Transaction. This requirement does not apply if the Mobile Payment Acceptance Solution used by the Merchant is both:
	
	  – Compliant with the Payment Card (PCI)-approved solution for commercial-off-the-shelf (COTS) devices
	
	  – Able to complete a payment Transaction through other means at the same location
	
	• Support Fallback Transactions[7]
	
	• Process the Transaction using data read from the Chip on a Chip Card unless any of the following apply, in which case the Transaction must be completed using data read from the Magnetic Stripe of a Chip Card:[7]
	
	  – The Chip is not EMV-Compliant.
	
	  – The Chip reader is inoperable.
	
	  – The Chip malfunctions during the Transaction or cannot be read. (In the Europe Region, the Chip-Reading Device must be capable of requiring an Online Authorization.)
	
	  – The Chip Transaction cannot be completed due to the absence of a mutually supported Application Identifier (AID).
	
	  If neither the Chip nor Magnetic Stripe of a Chip Card can be read and the Transaction is accepted using a paper voucher or key entry, the device must follow correct Fallback and acceptance procedures.[1]
	
	• Include an EMV Online Card Authentication Cryptogram and all data elements used to create it in all Online Authorization Requests for a Chip Transaction transmitted to VisaNet
	
	• Read an EMV-Compliant and VIS-Compliant Chip and not allow override of Chip Authorization controls by prompting for a Magnetic Stripe read[8]

Visa Core Rules and Visa Product and Service Rules

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements

	• Support terminal action codes
	
	• Include all mutually supported Payment Applications between the Chip and the device in the application selection process, and not discriminate between Payment Applications unless stipulated by Chip parameters or a Visa-approved application selection process
	
	• Act on the Cardholder Verification Method list,[9] unless otherwise specified
	
	• If using an active PIN pad, both:
	
	  – Comply with Visa encryption standards
	
	  – Be active for Visa Chip-initiated Transactions if it is active for other Chip-enabled payments
	
	• Have a PIN pad or a port capable of supporting a PIN pad and, if using an active PIN pad, comply with Visa encryption standards
	
	• If the device is equipped with only a PIN pad port or PIN pad is inactive for Chip-initiated Transactions, support software to ensure compliance with Visa encryption standards
	
	• Have the capability to have its Visa Public Keys replaced in an acceptable method by any Visa-specified date
	
	• Support Post-Issuance Application commands
	
	• If a PIN-only Chip-Reading Device, not display the Visa Brand Mark (excluding ATMs and Unattended Cardholder-Activated Terminals [UCATs] that accept only PINs for Cardholder Verification)
	
	• Prompt a Cardholder for a PIN only if required by the Chip, except for ATMs and offline-only UCATs, and devices deployed in the Europe Region that are always required to prompt for a PIN
	
	• Support "Plaintext Offline PIN" if it supports "Enciphered Offline PIN"
	
	• In the AP Region (Australia): All of the following:
	
	  – Accept both Online and Offline PIN
	
	  – For international Transactions support PIN bypass
	
	  – Ensure that a Domestic Transaction uses a PIN, except for:
	
	    ▪ A Transaction initiated with a Card that is not a PIN-Preferring Chip Card

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements
	▪ An Unattended Transaction, including an Unattended Transaction that does not qualify as a Visa Easy Payment Service (VEPS) Transaction ▪ A VEPS Transaction ● In the LAC Region (Brazil): If deployed after 18 November 2013, support Offline PIN Verification (except UCATs in parking lots/garages and vending machines) ● In the Canada Region: Support both: – "Plaintext Offline PIN" – "Enciphered Offline PIN" ● In the CEMEA Region: – Support both: ▪ For an Offline-Capable Chip-Reading Device, support both "Plaintext Offline PIN" and "Enciphered Offline PIN" ▪ For an Online-only Chip-Reading Device, support either ▪ "Enciphered Online PIN" ▪ Both "Plaintext Offline PIN" and "Enciphered Offline PIN" – Chip-Reading Devices may suppress their PIN capability for VEPS Transactions ● In the AP Region (Australia, Malaysia): Both: – If the device supports Cardholder application selection, do all of the following: ▪ Display to the Cardholder all mutually supported application names (application label or application preferred name) on the Card ▪ Display the application names in the order of the application priority set on the Card and use them to select the corresponding Payment Application ▪ If unable to display the application names in full, display at least the first 4 positions of the application names – If the device does not support Cardholder application selection, the Merchant must inform the Cardholder of the selected application before completing the Transaction ● In the Europe Region: All of the following: – Present options for mutually supported Payment Applications contained in the

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements
	Chip to the Cardholder, if the Cardholder has the ability to select the Payment Application
	– Support the terminal action codes and facilitates access to multiple accounts on a Chip Card
	– Support Static Data Authentication and Dynamic Data Authentication (optional for Online-only devices)
	– Either:
	▪ For an Online-only device that does not support both "Plaintext Offline PIN" and "Enciphered Offline PIN," support "Enciphered PIN Verified Online"
	▪ For an Online-capable device, support "Plaintext PIN Verified Offline" and "Enciphered PIN Verified Offline"
	– If deployed after 1 July 2008, accept PINs. This does not apply to the following:
	▪ A Merchant assigned MCC 4784 (Tolls and Bridge Fees)
	▪ A UCAT installed at a vehicle entrance gate at a ferry Merchant provided that the UCAT always requests Online Authorization and that PIN verification of Chip-initiated Transactions may be performed at attended gates at the same Merchant Outlet
	▪ A UCAT that accepts only Contactless Payment Devices
	▪ An Unattended Transaction that does not use MCC 4829, 6011, 6012, 6051, or 7995 and is below the maximum applicable Visa Easy Payment Service (VEPS) Transaction amount or, for MCC 4111, 4112, 4131, 4784, or 7523, EUR 100
Contactless Chip	• Be approved by EMVCo or Visa
	• If deployed after 1 May 2013, not limit the Transaction amount of a Contactless Transaction in a Face-to-Face Environment
	• If deployed on or after 16 October 2015,[10] forward to Visa the form factor indicator field, when provided by a Contactless Payment Device
	• In the AP Region (Australia): For International Transactions support PIN bypass
	• In the AP Region, Canada Region, CEMEA Region, LAC Region: If deployed on or before 1 January 2012, comply with the *Visa Contactless Payment Specification 2.0* or later[7] and be capable of processing a Transaction using the qVSDC transaction path and transmitting the resulting Chip data to VisaNet

Visa Core Rules and Visa Product and Service Rules

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements
	• In the AP Region and CEMEA Region: All of the following: – Comply with the *Visa Contactless Payment Specification 2.1.3* or later[11] or the equivalent EMV contactless kernel 3 – Be capable of processing a Transaction using the qVSDC transaction path and transmitting the resulting Chip data to VisaNet – Disable the device's Contactless Transaction limit – Enable the device's applicable Cardholder Verification Method (CVM) Transaction limit – Enable the device's applicable Contactless Chip Floor Limit – Support the application program ID (APID) – Include the form factor indicator in the Authorization Request and Clearing Record when provided by the Contactless Payment Device[10] – Not support the MSD transaction path • In the Canada Region and LAC Region: If deployed after 1 April 2014, comply with the *Visa Contactless Payment Specification 2.1.1* or later, or the equivalent EMV contactless kernel 3, and be capable of processing a Transaction using the qVSDC transaction path and transmitting the resulting Chip data to VisaNet • In the Canada Region: Not support the MSD transaction path • In the Europe Region: All of the following: – Be approved by Visa to process Contactless Transactions – If deployed on or before 13 September 2019, comply with the *Visa Europe Contactless Terminal Requirements and Implementation Guide* Version 1.3 – If deployed on or after 14 September 2019, comply with the *Visa Europe Contactless Terminal Requirements and Implementation Guide* Version 1.5 or later[12] – If not Contactless-only, be able to process other Chip-initiated Transactions – If not Contactless-only, support Online Authorization – Process a Transaction using the qVSDC path – Allow the Acquirer to update the following data fields: ▪ "Reader Contactless Floor Limit"

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements
	▪ "Reader CVM Required Limit"
	– Comply with either:
	▪ The *Visa Contactless Payment Specification Version 2.1.1* or later
	▪ The *EMV Contactless Specification for Payment Systems Book C-3*
	– If compliant with the *Visa Contactless Payment Specification Version 2.1* or later or the *EMV Contactless Specification for Payment Systems Book C-3*, do all of the following:
	▪ Set the "Reader CVM Required Limit" to the applicable Cardholder Verification Limit
	▪ Set the "Reader Contactless Floor Limit" to the applicable Proximity Payment Floor Limit
	▪ Not configure the "Reader Contactless Transaction Limit"
	– Include the form factor indicator in the Authorization Request and Clearing Record when provided by the Contactless Payment Device
	– If an ATM, support only Online Authorization
	– Be approved by Visa to process Contactless Transactions
	– Not accept a Transaction using the MSD transaction path
	• In the LAC Region: Comply with the Visa Contactless Payment Specification 2.1.3 or later, or the equivalent EMV contactless kernel 3, and be capable of processing a Transaction using the qVSDC transaction path and transmitting the resulting Chip data to VisaNet
	• For all Contactless Acceptance Devices in the US Region: All of the following:
	– Comply with the *Visa Contactless Payment Specification 2.1.1* or later
	– Actively enable the qVSDC transaction path
	– Not support the MSD transaction path
Contactless-Only	• Comply with *Section 5.7.2.2, Deployment of Contactless-Only Acceptance Devices*
	• Accept all Contactless Payment Devices
	• Not have a disabled contact Chip reader or Magnetic-Stripe slot
	• Include the following values in the Authorization Request and Clearing Record:

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements

	– POS Entry Mode code 07
	
	– POS terminal entry capability 8
	
	• If a Contactless-only Acceptance Device deployed by a Mass Transit Merchant is configured to always perform offline data authentication before allowing a Cardholder to access the transit services, all of the following:
	
	  – Be configured in the same transit mode or network to perform offline data authentication
	
	  – Support either real-time or deferred Online Authorization at all turnstiles, fare gates, or points of boarding
	
	  – **Effective through 14 April 2023** Support Visa contactless static data authentication and Dynamic Data Authentication
	
	  – **Effective 15 April 2023** Not support Visa contactless static data authentication
	
	  – **Effective 15 April 2023** Support Visa contactless Dynamic Data Authentication

Magnetic Stripe	• Transmit the entire unaltered contents of all data encoded on track 1 or track 2 of the Magnetic Stripe • Not erase or alter any Magnetic-Stripe encoding on a Card • For devices that can accept Cards with more than one Magnetic Stripe, be capable of processing and transmitting the payment data from the Visa Magnetic Stripe • In the AP Region (Australia, New Zealand): Allow PIN bypass for Domestic Transactions • In the Europe Region (United Kingdom): Retain the Card on receipt of a Pickup Response for a Magnetic Stripe-only Acceptance Device

Mobile Payment Acceptance Solution	In the Europe Region: All of the following:
	
	• Include a hardware accessory that must comply with all of the following:
	
	  – Be able to capture Cardholder and Card data
	
	  – Have an integrated Chip reader that is EMV-Compliant
	
	  – Support secure PIN entry
	
	  – Include "signature" in the Cardholder Verification Method
	
	  – Comply with the *Payment Card Industry (PCI) POS PIN Entry Device Security*

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements
	Requirements Version 2.0 or later, including the additional Secure Read and Exchange of Data (SRED) module requirements – Ensure the SRED module is enabled for point-to-point Cardholder data encryption • Have an integrated Magnetic Stripe-reader. This requirement does not apply if the Mobile Payment Acceptance Solution used by the Merchant is both: – Compliant with the Payment Card (PCI)-approved solution for commercial-off-the-shelf (COTS) devices – Able to complete a payment Transaction through other means at the same location • Not read or capture account data except via the hardware accessory • Identify the Transaction in the Authorization Request and Clearing Record
QR Code reader	• **Effective through 18 October 2019** Be deployed only in the US Region • Be deployed only in the AP Region • Comply with the *Visa QR Code Payment Specification (VQRPS)* • Use POS Entry Mode code 03 • Transmit Full-Chip Data to VisaNet
Unattended Cardholder-Activated Terminal (UCAT)	• Identify each Transaction as initiated by a UCAT • Display the Merchant name and customer service telephone number • If PIN-accepting, be capable of conveying an "invalid PIN – re-enter" message to the Cardholder • **Effective 15 October 2022** In the Canada Region: All of the following: – If capable of accepting PINs, both: ▪ Accept PINs ▪ Be capable of conveying all of the following messages to the Cardholder: ▪ Card invalid for this service ▪ Service unavailable now ▪ Invalid PIN – re-enter

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements

	– If the UCAT does not accept PINs, support "No CVM (Cardholder Verification Method) required"
	
	  – For a Chip-reading-only UCAT, all of the following:
	
	    ▪ Be EMV-Compliant
	
	    ▪ Ensure that Magnetic Stripe-only Cardholders are able to conduct Transactions at the same location
	
	    ▪ If a Card cannot be read and the UCAT is Offline-only, must not complete the Transaction using the Magnetic Stripe Data. If the UCAT is Online-only, may be capable of completing the Transaction using the Magnetic Stripe Data
	
	• In the Europe Region: All of the following:
	
	  – Support Fallback Transactions only if the UCAT has an integrated Chip and Magnetic Stripe-reader and Card capture capability, except in the United Kingdom where Fallback Transactions must not be processed
	
	  – If capable of accepting PINs, both:
	
	    ▪ Accept PINs
	
	    ▪ Be capable of conveying all of the following messages to the Cardholder:
	
	      ▪ Card invalid for this service
	
	      ▪ Service unavailable now
	
	      ▪ Invalid PIN – re-enter
	
	  – If the UCAT does not accept PINs, support "No CVM (Cardholder Verification Method) required"
	
	  – For a Chip-reading-only UCAT, all of the following:
	
	    ▪ Be EMV-Compliant
	
	    ▪ Ensure that Magnetic Stripe-only Cardholders are able to conduct Transactions at the same location
	
	    ▪ If a Card cannot be read and the UCAT is Offline-only, must not complete the Transaction using the Magnetic Stripe data (if the UCAT is Online-only, may be capable of completing the Transaction using the Magnetic Stripe data)
	
	  – In the Europe Region (United Kingdom): Both:

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements

	• For an Automated Fuel Dispenser (AFD), not accept Visa Electron Cards
	• For a Magnetic Stripe-read Transaction, not support online PIN Verification
	
	● If Online-capable, for Chip-initiated and Contactless Transactions, support "No CVM required"
	
	● Require PIN or Consumer Device Cardholder Verification Method for Quasi-Cash Transactions
	
	● If used for the purchase of gambling services, all of the following:
	  – Display the Merchant location
	  – Display the terms and conditions (including rules of play, odds of winning, and pay-out ratios)
	  – Before initiating the Transaction, allow the Cardholder to cancel the Transaction
	
	● Follow all applicable Point-of-Transaction acceptance requirements when accepting payment for goods or services, and follow ATM requirements when dispensing cash

1   If neither the Chip nor Magnetic Stripe of a Card can be read by a Chip-enabled device, a Merchant is not required to key enter a Transaction.

2   In the LAC Region (Brazil): This does not apply.

3   In the AP Region, CEMEA Region: This does not apply to a Point-of-Transaction Terminal installed at a Branch or an ATM.

4   In the Europe Region: This does not apply to Mobile Acceptance Terminals used by a Merchant that does not trade in a fixed location, Point-of-Transaction Terminals installed at a Branch, Automated Fuel Dispensers, or ATMs.

5   **Effective through 12 October 2021** In the LAC Region: This does not apply to new Mobile Acceptance Terminals, integrated fuel dispensers, electronic cash registers, or ATMs.

6   **Effective 1 April 2023 through 31 March 2025** In the LAC Region: This does not apply to Mobile Acceptance Terminals, integrated fuel dispensers, electronic cash registers, or ATMs.

7   In the AP Region (Japan): This does not apply to ATMs.

8   In the AP Region (Japan): This does not apply to Account Number Verification Transactions processed as Magnetic-Stripe Transactions.

9   **Effective through 17 April 2020** This does not apply to a Transaction that takes place at a Compliant Chip Card Reading Device, at which the Merchant may process a Transaction without a Cardholder signature (except in the AP Region [Japan, Philippines] or where applicable laws or regulations require a Cardholder Verification Method to be captured, which may include a signature).
Effective 18 April 2020 This does not apply to a Transaction that takes place at a Compliant Chip Card Reading

Table 5-9: Acceptance Device Requirements (continued)

Acceptance Device Type	Requirements
	Device, at which the Merchant may process a Transaction without a Cardholder signature (except where applicable laws or regulations require a Cardholder Verification Method to be captured, which may include a signature).
	[10] In the AP Region (Japan): 1 October 2018
	[11] In the AP Region (Japan): This requirement does not apply to Visa Touch readers.
	[12] In the Europe Region (Czech Republic, Hungary, Poland, Slovakia): All Acceptance Devices must comply with the *Visa Europe Contactless Terminal Requirements and Implementation Guide* Version 1.5 or later.

ID# 0028045	Edition: Apr 2020 | Last Updated: Apr 2020

5.7.1.2   Visa Electron Card Acceptance Requirements

A Visa Electron Merchant must process Transactions using:

- An Acceptance Device with Electronic Capability
- In the CEMEA Region (South Africa): A PIN-enabled Acceptance Device

ID# 0003658	Edition: Apr 2020 | Last Updated: Oct 2014

5.7.2   Chip Acceptance Device Requirements

5.7.2.1   Chip Acceptance Device Testing Requirements

An Acquirer must successfully complete testing of a Chip Acceptance Device, as follows:

Table 5-10: Chip Acceptance Device Testing Requirements

Acceptance Device Type	Testing Tool	When Required	Submission Requirements
Chip-Reading Device	Acquirer Device Validation Toolkit (ADVT)	• Before deploying or upgrading a Chip-Reading Device	• Submit test results using the Chip Compliance Reporting Tool (CCRT)[1] • Not submit ADVT test results for a device containing a kernel or interface module (IFM) that

Table 5-10: Chip Acceptance Device Testing Requirements (continued)

Acceptance Device Type	Testing Tool	When Required	Submission Requirements
			has expired
Contactless Chip-Reading Device	Either: • Contactless Device Evaluation Toolkit (CDET) • In the Europe Region, Visa payWave Test Tool (VpTT)	Before deploying either a: • New Contactless Chip-Reading Device • Existing Contactless Chip-Reading Device that has undergone a significant hardware or software upgrade	Submit test results using: • CCRT[1] • In the Europe Region: VpTT
In the Europe Region: Mobile Payment Acceptance Solution	• Acquirer Device Validation Toolkit (ADVT) • Visa payWave Test Tool (VpTT)	Before deploying a new Mobile Payment Acceptance Solution that has not previously been validated by Visa and tested for the same implementation by a different Acquirer	• Submit test results with the word "Mobile" in the test result description • Submit PCI Secure Read and Exchange of Data (SRED) certification details • For devices with a Contactless reader, submit the VpTT results
[1] A centralized, server-based, online solution for the systematic reporting of ADVT and CDET test results. In the US Region: Not required for Acquirers participating in the Chip Acquirer Self Accreditation program.			

5.7.2.2   Deployment of Contactless-Only Acceptance Devices

A Merchant may deploy a Contactless-only Acceptance Device only as follows:

Table 5-11: Conditions for Deployment of Contactless-Only Acceptance Devices (Effective through 17 April 2020)

Region/Country/Territory	Transaction Type	Maximum Transaction Amount	Acceptance Requirements
All	Unattended Transactions at a transit Merchant turnstile, fare gate, or point of boarding (MCC 4111, 4112, or 4131)	None	A passenger vehicle (for example: bus, ferry) with a Contactless-only Acceptance Device must accept all Contactless Payment Devices. All Cards must be accepted at other transit Merchant Outlets.
AP Region (Australia, Hong Kong, Japan, Malaysia, Myanmar, New Zealand, Singapore, Taiwan), Canada Region, CEMEA Region (Georgia, Russia), Europe Region, LAC Region (Costa Rica)	Face-to-Face or Unattended Transactions for toll payments (MCC 4784)	Less than or equal to the limits specified in *Section 5.9.11.2, Maximum Transaction Amounts for Visa Easy Payment Service (VEPS) Transactions and Transactions at Certain Contactless-Only Acceptance Devices*	All Contactless Payment Devices must be accepted at the Merchant Outlet.
	Face-to-Face or Unattended Transactions for donations	None	All Contactless Payment Devices must be accepted at the Merchant Outlet.
	Other Unattended Transactions, except: • ATM Cash Disbursements • Automated Fuel Dispenser Transactions • Transit Merchant Transactions not	Less than or equal to the limits specified in *Section 5.9.11.2, Maximum Transaction Amounts for Visa Easy Payment Service (VEPS) Transactions and Transactions at Certain*	All Contactless Payment Devices must be accepted at the Merchant Outlet.

Table 5-11: Conditions for Deployment of Contactless-Only Acceptance Devices (Effective through 17 April 2020) (continued)

Region/Country/Territory	Transaction Type	Maximum Transaction Amount	Acceptance Requirements
	otherwise specified • Quasi-Cash Transactions	*Contactless-Only Acceptance Devices*	
	Other Face-to-Face Transactions	None	All Cards must be accepted at the Merchant Outlet.

Table 5-12: Conditions for Deployment of Contactless-Only Acceptance Devices (Effective 18 April 2020)

Transaction Type	Maximum Transaction Amount	Acceptance Requirements (in addition to applicable requirements in *Section 5.7.11, Acceptance Device Requirements*)
Face-to-Face Transactions:		
For donations	None	All Cards must be accepted on the Merchant's website or application.[1]
For toll payments (MCC 4784)	Less than or equal to the limits specified in *Section 5.9.11.2, Maximum Transaction Amounts for Visa Easy Payment Service (VEPS) Transactions and Transactions at Certain Contactless-Only Acceptance Devices*	All Cards must be accepted at other Acceptance Devices at the Merchant Outlet.
To enable faster customer throughput ("queue-busting")[2]	None	All Cards must be accepted at other Acceptance Devices at the Merchant Outlet. If all Cards are not able to be accepted at the Merchant Outlet, the Merchant Outlet must not deploy a Contactless-only Acceptance Device.
Unattended Transactions:		

Table 5-12: Conditions for Deployment of Contactless-Only Acceptance Devices (Effective 18 April 2020) (continued)

Transaction Type	Maximum Transaction Amount	Acceptance Requirements (in addition to applicable requirements in *Section 5.7.11, Acceptance Device Requirements*)
At a Mass Transit Merchant turnstile, fare gate, or point of boarding	None	A passenger vehicle (for example: bus, ferry) with a Contactless-only Acceptance Device must accept all Contactless Payment Devices. All Cards must be accepted at other Mass Transit Merchant Outlets.
For: • Electric vehicle charging (MCC 5552) • Parking (MCC 7523)	None	All Cards must be accepted at other Acceptance Devices at the Merchant Outlet or on the Merchant's website or application.
In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: For all other Transactions, except: • ATM Cash Disbursements • Automated Fuel Dispenser Transactions • Transit Merchant Transactions not otherwise specified • Quasi-Cash Transactions	Less than or equal to the limits specified in *Section 5.9.11.2, Maximum Transaction Amounts for Visa Easy Payment Service (VEPS) Transactions and Transactions at Certain Contactless-Only Acceptance Devices*	If the Unattended Cardholder-Activated Terminal (UCAT) is capable of processing Transactions above the applicable Visa Easy Payment Service (VEPS) limit, all Cards must be accepted at the UCAT. In addition, for toll payments, all Cards must be accepted at other Acceptance Devices at the Merchant Outlet or on the Merchant's website or application.
[1] **Effective 17 April 2021** for Acceptance Devices deployed on or before 18 April 2020		
[2] In the US Region: **Effective 17 April 2021**		

ID# 0026670   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.7.2.3   PIN-Entry Bypass Prohibition – Canada Region

In the Canada Region: An Acquirer must ensure that PIN entry on a Compliant Chip-Reading Device with a PIN Entry Device cannot be bypassed by the Acquirer, the Merchant, or an agent of the Acquirer or Merchant.

ID# 0004863	Edition: Apr 2020	Last Updated: Oct 2014

5.7.3   Unattended Cardholder-Activated Terminals – Transaction Cancellation

5.7.3.1   Acquirer Cancellation of Transactions at Unattended Cardholder-Activated Terminals

If an Unattended Cardholder-Activated Terminal allows an Acquirer to cancel a Transaction, the Acquirer may use this function without Issuer permission only after one of the following:

ID# 0025727	Edition: Apr 2020	Last Updated: Oct 2014

5.8   Merchant Authorization Requirements

5.8.1   Transactions Requiring Authorization

5.8.1.1   Floor Limits and Requirement to Authorize Transactions

A Merchant must request Online Authorization if a Transaction amount exceeds the Floor Limit.

For Transactions below the Floor Limit, Authorization is not required for a Magnetic Stripe Transaction and Offline Authorization is permitted for a Chip-initiated Transaction.

Regardless of the Floor Limit, a Merchant must request Online Authorization if any of the following:

- The Cardholder presents an Expired Card.
- The Service Code requires Online Authorization or the Chip requests Online Authorization.
- The Transaction is any of the following:
  - A Transaction that includes Cash-Back
  - A Cash Disbursement
  - A Credit Transaction, as specified in *Section 5.11.1.1, Merchant Processing of Credits to Cardholders*
  - A Debt repayment Transaction

- – A Fallback Transaction
- – A Quasi-Cash Transaction
- In the Europe Region: The Transaction is at a Merchant assigned one of the following MCCs:
  - – MCC 5451 (Dairy Products Stores)
  - – MCC 5921 (Package Stores – Beer, Wine, and Liquor)
  - – MCC 5994 (News Dealers and Newsstands)
  - – MCC 7297 (Massage Parlors)
  - – MCC 7995 (Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks)

ID# 0008901	Edition: Apr 2020	Last Updated: Apr 2020

5.8.2 Transaction Amount-Related Authorization Requirements

5.8.2.1 Merchant Requirement to Check the Card Recovery Bulletin (CRB)

A Merchant must check the appropriate Card Recovery Bulletin (CRB) if the Transaction amount is below the Floor Limit.

The Merchant is not required to check the CRB if the Transaction occurs at a Chip-Reading Device.

ID# 0003010	Edition: Apr 2020	Last Updated: Apr 2018

5.8.3 Non-Standard Authorizations

5.8.3.1 Authorization Amount Requirements

A Merchant must submit an Authorization Request for either:

- The final Transaction amount
- A different amount or amounts if the final Transaction amount is not known, and the Merchant or Transaction type is included in and complies with *Table 5-13, Special Authorization Request Allowances and Requirements*[1]

Table 5-13: Special Authorization Request Allowances and Requirements

Merchant / Transaction Type	Allowed Type and Amount of First or Only Authorization Request	Incremental Authorization Request(s) Allowed?	Other Requirements and Restrictions
Card-Absent Environment Aggregated Transactions	An amount up to and including USD 15 (or local currency equivalent)	No	The total amount of the Initial Authorization Request must not exceed USD 15 (or local currency equivalent).
Any of the following Merchants: • Aircraft rental • Bicycle rental • Boat rental • Equipment rental • Motor home rental • Motorcycle rental • Trailer park or campground	Estimated Authorization Request[2]	Yes[3]	The Merchant must not include an amount to cover potential damage or an insurance deductible. When submitting the first Estimated Authorization Request, the Merchant must inform the Cardholder both: • That the Authorization Request is not final and that there may be subsequent Authorization Requests • Of the amount of the Estimated Authorization Request
Automated Fuel Dispenser (AFD) Transactions (MCC 5542)	One of the following: • Status Check Authorization[4] • Real-Time Clearing preauthorization request, not exceeding USD 500 (or local currency equivalent), and the actual Transaction amount (Completion Message) within 2 hours of the preauthorization	No	A Status Check Authorization is equivalent to an Approval Response for an amount up to and including: • For a Transaction in the AP Region (Japan), JPY 15,000[6] • For a Transaction in the US Region: Either: – **Effective 17 October 2020** For a Chip-initiated Transaction that

Table 5-13: Special Authorization Request Allowances and Requirements (continued)

Merchant / Transaction Type	Allowed Type and Amount of First or Only Authorization Request	Incremental Authorization Request(s) Allowed?	Other Requirements and Restrictions
	request • An amount not exceeding USD 150 (or local currency equivalent)[5] In the Europe Region: An amount based on the Merchant's maximum dispensable fuel amount, not exceeding EUR 150 (or local currency equivalent). When the final amount is known, the Acquirer must send an Acquirer Confirmation Advice equal to the amount transmitted in the Clearing Record.		contains a Partial Authorization indicator, either: ▪ For a Visa Fleet Card Transaction, USD 350 ▪ For all other Transactions, USD 125 – For all other Transactions, either:[6] ▪ For a Visa Fleet Card Transaction, USD 150 ▪ For all other Transactions, USD 100 • For other Transactions, either:[6] – For a Chip-initiated Transaction with a PIN, USD 100 (or local currency equivalent) – For all other Transactions, USD 75 (or local currency equivalent)
Card-Absent Environment Transactions (except Installment Transactions, Advance Payments, Recurring Transactions, and Transactions classified with MCC 4121)	Price of merchandise or services, including shipping costs and applicable taxes	No	An additional Authorization is not required if the Transaction amount is within 15% of the authorized amount.[6,7]

Visa Product and Service Rules

5 Acceptance

Visa Core Rules and Visa Product and Service Rules

Table 5-13: Special Authorization Request Allowances and Requirements (continued)

Merchant / Transaction Type	Allowed Type and Amount of First or Only Authorization Request	Incremental Authorization Request(s) Allowed?	Other Requirements and Restrictions
Cruise Lines Lodging Merchants	Estimated Authorization Request[2]	Yes[3]	The Merchant must not include an amount to cover potential damage or an insurance deductible. When submitting the first Estimated Authorization Request, the Merchant must inform the Cardholder both: • That the Authorization Request is not final and that there may be subsequent Authorization Requests • Of the amount of the Estimated Authorization Request The Merchant is not required to submit a final Incremental Authorization Request if the final Transaction amount is no more than 15% higher than the sum of the authorized amounts.[6]
Merchants classified with MCC: • 4121 (Taxicabs and Limousines) • 5814 (Fast Food Restaurants) • 7230 (Beauty and Barber Shops)	An amount equal to the final Transaction amount (excluding an expected tip or service amount)	No	An additional Authorization is not required if the final Transaction amount (including tip or service amount) is within 20%[7] of the authorized amount.

Visa Product and Service Rules

5 Acceptance

Visa Core Rules and Visa Product and Service Rules

Table 5-13: Special Authorization Request Allowances and Requirements (continued)

Merchant / Transaction Type	Allowed Type and Amount of First or Only Authorization Request	Incremental Authorization Request(s) Allowed?	Other Requirements and Restrictions
• 7298 (Health and Beauty Spas)			
Card-Absent Environment Transactions classified with MCC 4121 (Taxicabs and Limousines)	Estimated Authorization Request[2]	Yes[3]	The Merchant must not include an amount to cover a tip if the Cardholder has not determined the amount of the tip. An additional Authorization is not required if the final Transaction amount (including tip or service amount) is within 20%[7] of the authorized amount.
Card-Absent Environment Transactions classified with MCC 5411 (Grocery Stores and Supermarkets)	Estimated Authorization Request[2]	Yes[3]	An additional Authorization is not required if the Transaction amount is within 15% of the authorized amount.
Merchants classified with MCC: • 5812 (Eating Places and Restaurants) • 5813 (Drinking Places [Alcoholic Beverages – Bars, Taverns, Nightclubs, Cocktail Lounges, and Discotheques])	Either: • An amount equal to the final Transaction amount (excluding an expected tip or service amount) • Initial Authorization Request[2] for an amount equal to what the Cardholder has ordered (excluding expected tip or service amount)	Yes, only for additional goods or services ordered[3]	An Incremental Authorization Request or additional Authorization Request is not required if the final Transaction amount (including tip or service amount) is within 20%[6] of the authorized amount. If the Merchant submits a final Authorization Request for the final Transaction amount before a tip or service amount is added, an additional

Table 5-13: Special Authorization Request Allowances and Requirements (continued)

Merchant / Transaction Type	Allowed Type and Amount of First or Only Authorization Request	Incremental Authorization Request(s) Allowed?	Other Requirements and Restrictions
			Authorization Request is not required if the final Transaction amount (including tip or service amount) is within 20% of the authorized amount.
Merchants classified with MCC: • 7996 (Amusement Parks, Circuses, Carnivals, and Fortune Tellers) • 5552 (Electric Vehicle Charging) • 7523 (Parking Lots, Parking Meters and Garages)	Estimated Authorization Request[2]	Yes[3]	When submitting the first Estimated Authorization Request, the Merchant must inform the Cardholder both: • That the Authorization Request is not final and that there may be subsequent Authorization Requests • Of the amount of the Estimated Authorization Request
A Transaction or an Aggregated Transaction at a turnstile, fare gate, or point of boarding at Merchants classified with MCC: • 4111 (Local and Suburban Commuter Passenger Transportation, Including Ferries) • 4112 (Passenger Railways) • 4131 (Bus Lines)	Initial Authorization Request[2] equal to the price of the cheapest journey a Cardholder can take	Yes[3]	The total amount of the Initial Authorization Request and any Incremental Authorization Requests must not exceed USD 25 (or local currency equivalent) (in the US Region, USD 15).

Table 5-13: Special Authorization Request Allowances and Requirements (continued)

Merchant / Transaction Type	Allowed Type and Amount of First or Only Authorization Request	Incremental Authorization Request(s) Allowed?	Other Requirements and Restrictions
This does not apply to a Mass Transit Transaction.			
Unattended Transactions at Merchants classified with MCC 7211 (Laundries – Family and Commercial)	An amount not exceeding USD 10 (or local currency equivalent)	No	The Merchant must notify the Cardholder of the Authorization Request amount and give the Cardholder the opportunity to cancel the Transaction.
Unattended Transactions at Merchants classified with MCC: • 7338 (Quick Copy, Reproduction, and Blueprinting Services) • 7542 (Car Washes) • 7841 (DVD/Video Tape Rental Stores)	An amount not exceeding USD 15 (or local currency equivalent)	No	The Merchant must notify the Cardholder of the Authorization Request amount and give the Cardholder the opportunity to cancel the Transaction.
Unattended Transactions for the sale of food or beverages	An amount not exceeding USD 5 (or local currency equivalent)	No	The Merchant must notify the Cardholder of the Authorization Request amount and give the Cardholder the opportunity to cancel the Transaction.
Vehicle Rental Merchants	Estimated Authorization Request[2]	Yes[3]	The Merchant must not include an amount to cover potential damage or an insurance deductible. When submitting the first

Table 5-13: Special Authorization Request Allowances and Requirements (continued)

Merchant / Transaction Type	Allowed Type and Amount of First or Only Authorization Request	Incremental Authorization Request(s) Allowed?	Other Requirements and Restrictions
			Estimated Authorization Request, the Merchant must inform the Cardholder both: • That the Authorization Request is not final and that there may be subsequent Authorization Requests • Of the amount of the Estimated Authorization Request The Merchant is not required to submit a final Incremental Authorization Request if the final Transaction amount is no more than the greater of either: • The sum of the authorized amounts plus 15%[6] • The sum of the authorized amounts plus USD 75 (or local currency equivalent)[4,6]

[1]   This does not apply to a Visa Purchasing Card enrolled in Authorization and Settlement Match.

[2]   The Merchant must use the Estimated/Initial Authorization Request indicator.

[3]   The Merchant must use the Incremental Authorization Request indicator and the same Transaction Identifier for all Authorization Requests.

[4]   This does not apply to a Transaction involving a Merchant in the Europe Region.

[5]   This does not apply to a Transaction involving a Merchant in the US Region.

[6]   This does not apply if the last Authorization obtained was a Partial Authorization.

[7]   This does not apply if the Transaction is a Commercial Payables Transaction completed with a Visa Purchasing Card.

ID# 0025596	Edition: Apr 2020	Last Updated: Apr 2020

5.8.4   Merchant Authorization Processing

5.8.4.1   Mail/Phone Order and Electronic Commerce Expiration Date in Authorization

A Mail/Phone Order Merchant and an Electronic Commerce Merchant (for a Non-Secure Transaction and Non-Authenticated Security Transaction) must attempt to obtain a Visa Card expiration date and submit it as part of the Authorization Request.

ID# 0003129	Edition: Apr 2020	Last Updated: Oct 2014

5.8.4.2   Prohibition against Split Transaction

A Merchant must not split a transaction by using 2 or more Transaction Receipts, except for the following:

- Advance Payment
- Ancillary Purchase Transaction
- Individual Airline ticket
- Individual Cruise Line ticket
- Installment Transaction
- Original Credit Transaction
- A transaction in which part of the amount is paid with a Visa Card and the other part paid with another Visa Card or other form of payment
- In the Canada Region, US Region: Transaction that includes a Service Fee
- In the US Region: Individual passenger railway ticket

ID# 0008603	Edition: Apr 2020	Last Updated: Apr 2020

5.8.4.3   Single Authorization Request for Multiple Clearing Transactions

A Merchant may obtain a single Authorization and submit multiple Clearing Records only if one of the following:

- The Merchant is an Airline, a Cruise Line, or a US railway Merchant.
- The Merchant is a Card-Absent Environment Merchant that ships goods, and all of the following:
  - The purpose is to support a split shipment of goods.
  - The Transaction Receipts associated with each shipment contain:
    - The same Payment Credential and expiration date
    - The same Merchant Outlet name
  - The Merchant discloses to the Cardholder the possibility of multiple shipments on its website and/or application or in writing.
  - With each shipment, the Merchant notifies the Cardholder of the Transaction amount of the shipment.
  - The Transaction is not completed with a Visa Commercial Card enrolled in Authorization and Settlement Match.
- In the LAC Region (Brazil): The Transaction is a domestic Installment Transaction

The Acquirer must use a Multiple Clearing Sequence Number.

ID# 0027756   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.8.4.4   Deferred Authorization Merchant Requirements

Effective through 16 April 2021 An Acquirer that sends an Authorization Request for a Transaction that cannot be submitted at the time of the Transaction due to a connectivity, system issue, or other limitations must both:

- Include a deferred Authorization indicator in the Authorization Request
- Obtain an Authorization as follows:
  - For MCC 4111, MCC 4112, or MCC 4131, within 4 days of the Transaction Date
  - For all other MCCs, within 24 hours of the Transaction Date

Effective 17 April 2021 An Acquirer or Merchant that sends an Authorization Request for a Transaction that cannot be submitted at the time of the Transaction due to a connectivity, system issue, or other limitations must both:

- Include a deferred Authorization indicator in the Authorization Request
- Obtain an Authorization as follows:
  - For MCC 4111, MCC 4112, or MCC 4131, within 4 days of the Transaction Date
  - For all other MCCs, within 24 hours of the Transaction Date

ID# 0030061   Edition: Apr 2020 | Last Updated: Apr 2019

5.8.4.5   Approval Response Validity Timeframes

An Approval Response is valid for a Transaction completed as follows:

Table 5-14: Approval Response Validity Periods

Transaction Type	Approval Response is valid for a Transaction Date:[1]
Aggregated Transaction in a Card-Absent Environment	No later than 7 calendar days from the date on which the first Authorization Request received an Approval Response
In-Transit Transaction	Within 24 hours of the Approval Response (Authorization may occur after the Transaction is completed) An Authorization Request for an In-Transit Transaction may occur while in transit or at the final destination. The Merchant must obtain Authorization within 24 hours of the passenger vehicle reaching its final destination.
• Installment Transaction • Advance Payment • Recurring Transaction • Unscheduled Credential-on-File Transaction • Card-Absent Environment Transactions classified with MCC 4121 (Taxicabs and Limousines) initiated with an Estimated Authorization Request	That is the day of the Approval Response[2]
Mass Transit Transaction	No later than 3 calendar days from the date of the Approval Response
Transaction (excluding a Mass Transit Transaction) initiated with an Initial Authorization Request at a turnstile, fare gate, or point of boarding at a transit Merchant classified with MCC 4111, 4112, or 4131	No later than 7 calendar days (in the US Region, 3 calendar days) from the date of the Approval Response to the Initial Authorization Request. Any Incremental Authorization Requests do not extend this timeframe.

Table 5-14: Approval Response Validity Periods (continued)

Transaction Type	Approval Response is valid for a Transaction Date:[1]
Transaction initiated with an Estimated Authorization Request at any of the following Merchants: • Aircraft rental • Bicycle rental • Boat rental • Equipment rental • Motor home rental • Motorcycle rental • Trailer parks and campgrounds	No later than 7 calendar days from the date of the Approval Response to the Estimated Authorization Request. Any Incremental Authorization Requests do not extend this timeframe.
Transaction initiated with an Estimated Authorization Request at any of the following Merchants: • Cruise Line • Lodging Merchant • Vehicle Rental Merchant	No later than 31 calendar days from the date of the Approval Response to the Estimated Authorization Request. Any Incremental Authorization Requests do not extend this timeframe.
Other Card-Absent Environment Transactions	No later than 7 calendar days from the date of the Approval Response
Other Card-Present Environment Transactions	That is the day of the Approval Response
[1] As specified in *Section 7.7.1.2, Transaction Date Limits*	
[2] In the LAC Region (Brazil): This does not apply to a domestic Installment Transaction.	

The Authorization date and the Transaction Date are each counted as one day.

ID# 0029524   Edition: Apr 2020 | Last Updated: Apr 2020

5.8.4.6   Merchant Submission of Authorization Reversals

A Merchant must submit an Authorization Reversal, as follows:[1]

Table 5-15: Authorization Reversal Requirement

Transaction	Reversal Amount	Reversal Timeframe
For a completed Transaction initiated with an Estimated Authorization Request at a Cruise Line, Lodging Merchant, or Vehicle Rental Merchant, and the final Transaction amount is more than 15% below the sum of the authorized amounts	Difference between the final Transaction amount and sum of the authorized amounts	Within 24 hours of Transaction completion
For all other completed Transactions, if the final Transaction amount is less than the sum of the authorized amounts	Difference between the final Transaction amount and sum of the authorized amounts	Within 24 hours of Transaction completion
For all other Approval Responses, if a Transaction is not completed	Authorized amount or amounts	Within 24 hours of the earlier of either: • When the Transaction was cancelled or the Cardholder decided to pay by other means • The end of the Approval Response validity period, as specified in *Section 5.8.4.5, Approval Response Validity Timeframes*

When a Merchant submits an Incremental Authorization Request, the Merchant may reverse multiple authorized amounts with a single Authorization Reversal only if it uses the same Transaction Identifier for all Authorization Requests and the Authorization Reversal.

[1]   These requirements do not apply to Automated Fuel Dispenser Transactions in the US Region or in the Europe Region.

ID# 0025597   **Edition: Apr 2020 | Last Updated: Oct 2019**

5.8.4.7   Prohibition of Magnetic Stripe-Read Authorization Requests from Visa Debit Category Cards – Canada Region

In the Canada Region: A Visa Debit Acquirer must not process a Magnetic Stripe-read Authorization Request from a domestic Visa Debit Category Card.

ID# 0025968   Edition: Apr 2020 | Last Updated: Apr 2020

5.9   Specific Acceptance Environments and Procedures

5.9.1   Cash, Cash Equivalents, and Prepaid

5.9.1.1   Manual Cash Disbursement Requirements

If a Member makes Manual Cash Disbursements to other Issuers' Cardholders, it must do so in a uniform manner for all Visa products properly presented.

In the Canada Region, US Region: A Member authorized to make Cash Disbursements must make Manual Cash Disbursements to Cardholders of other Issuers' Prepaid Cards at all of its Branches.

A Member may make Manual Cash Disbursements through the offices of its related companies only if all of the following:

- The companies are primarily engaged in providing financial services to the public.

- The Member or the Member's holding company wholly owns the company.

- Visa has given the Member prior approval.

ID# 0006851   Edition: Apr 2020 | Last Updated: Apr 2020

5.9.1.3   Manual Cash Disbursement – Acquirer Access Fee

In the AP Region (except Australia and Thailand), CEMEA Region, Europe Region, LAC Region (except Puerto Rico): An Acquirer must not impose an Access Fee on a domestic Manual Cash Disbursement unless applicable laws or regulations expressly require that the Acquirer be permitted to assess an Access Fee.

If an Acquirer assesses an Access Fee on a Manual Cash Disbursement, it must do all of the following:

- Disclose to the Cardholder the Access Fee before it is assessed and provide the Cardholder the opportunity to cancel the Manual Cash Disbursement

- Assess the Access Fee as a fixed and flat fee

- Assess the same Access Fee on all Visa products, regardless of Issuer

- Not assess an Access Fee on a Manual Cash Disbursement conducted with a Card issued in the Europe Region (unless applicable laws and regulations expressly require that the Acquirer be permitted to assess an Access Fee)

- In the Canada Region and US Region: Not assess an Access Fee on a Manual Cash Disbursement conducted with a domestic Prepaid Card

- Include the Cash Disbursement and Access Fee amounts in the same Clearing Record and identify the Access Fee separately

ID# 0028922   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.9.1.4   Cash-Back Requirements

In addition to the requirements for each country/Region in *Table 5-16, Cash-Back Requirements,* a Cash-Back Transaction must comply with all of the following:

- Be authorized Online

- Be completed as a domestic Retail Transaction in a Face-to-Face Environment

- Uniquely identify the Cash-Back portion of the Transaction amount

- Be processed in the Merchant's local currency

A Member must not process a credit refund or Credit Transaction Receipt for the Cash-Back component of a Transaction.

Table 5-16: Cash-Back Requirements

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
AP Region					
Australia	Must be available	USD 998 (or local currency equivalent)	Debit Card	Must contain a PIN or Consumer Device Cardholder Verification Method (CDCVM)	Must not be a Fallback Transaction
India	Must be available	Cash-Back disbursements must not exceed the daily Cash-Back limit	Only products permitted by the Reserve Bank of India	Must contain a PIN or CDCVM	N/A

Table 5-16: Cash-Back Requirements (continued)

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
		per Card specified by the Reserve Bank of India			
Japan	Not allowed	JPY 20,000	Debit Card	Must contain a PIN or CDCVM	Must not be a Fallback Transaction
Malaysia	Not allowed	MYR 500	• Debit Card • Reloadable Prepaid Card	Must contain a PIN or CDCVM	Must not be a Fallback Transaction
Sri Lanka	Not allowed	LKR 5,000	• Debit Card • **Effective through 12 April 2024** Electron Card	Must contain a PIN or CDCVM	N/A
Canada Region					
Canada	Not allowed	USD 200 (or local currency equivalent)	• Debit Card • Reloadable Prepaid Chip and PIN-enabled Card	Must contain a PIN or CDCVM	• All Acquirers and their processors must support Cash-Back at the POS • All Acquirers, Issuers, and Merchants must participate in Partial Authorization

Table 5-16: Cash-Back Requirements (continued)

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
CEMEA Region					
Botswana, Kenya, Ghana, Malawi, Mauritius, Mozambique, Rwanda, Serbia, Seychelles, Tanzania, Uganda, Ukraine, Zambia, Zimbabwe	Not allowed	USD 200 (or local currency equivalent)	• Debit Card • Reloadable Prepaid Card	Must contain a PIN or CDCVM	• All Acquirers and their processors must support Cash-Back at the POS • Partial Authorization not allowed
Egypt	Not allowed	EGP 500	• Debit Card • Reloadable Prepaid Card	Must contain a PIN or CDCVM	• All Acquirers and their processors must support Cash-Back at the POS • Partial Authorization not allowed
Russia	Not allowed	USD 200 (or local currency equivalent)	• Credit Card • Debit Card • Reloadable Prepaid Card	Must contain a PIN or CDCVM	• All Acquirers and their processors must support Cash-Back at the POS • Partial Authorization not allowed • Must not be a

Table 5-16: Cash-Back Requirements (continued)

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
					Fallback Transaction • Cash-Back at the POS is not allowed at a Merchant Outlet classified with the following MCC: – 3000 – 3200 – 3351 – 3500 – 4511 – 4784 – 4829 – 5542 – 5944 – 6012 – 6051 – 6211 – 6540 – 7512 – 7513 – 7519 – 7523 – 7995
South Africa	Allowed	Cash-Back Transaction	• Credit Card • Debit Card	Must contain a PIN or CDCVM	Partial Authorization

Table 5-16: Cash-Back Requirements (continued)

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
		amount must not exceed ZAR 5,000	• Reloadable Prepaid Card		not allowed
Europe Region					
Austria	Not allowed	EUR 200	• Debit Card	Must contain a PIN or CDCVM	N/A
Bulgaria	Not allowed	BGN 50	• Credit Card • Debit Card • **Effective through 12 April 2024** Electron Card	Must contain a PIN or CDCVM	N/A
Czech Republic	Not allowed	CZK 3,000	• Credit Card • Debit Card • **Effective through 12 April 2024** Electron Card	Must contain a PIN or CDCVM	N/A
Denmark	Not allowed	N/A	Debit Card	Must contain a PIN or CDCVM	N/A
Finland	Not allowed	EUR 400	• Credit Card • Debit Card • **Effective through 12 April 2024** Electron Card	Must contain a PIN or CDCVM	N/A

Table 5-16: Cash-Back Requirements (continued)

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
Germany	Not allowed	EUR 200	• Credit Card • Debit Card	Must contain a PIN or CDCVM	N/A
Greece	Not allowed (must be in conjunction with a purchase of at least EUR 10)	EUR 50 (per Card, per day)	• Credit Card • Debit Card • **Effective through 12 April 2024** Electron Card	Must contain a PIN or CDCVM	Merchant Outlet must be classified with MCC 5311 or 5411
Italy	Not allowed	EUR 100	• Debit Card • **Effective through 12 April 2024** Electron Card • Reloadable Prepaid Card	Must contain a PIN or CDCVM	N/A
Poland	Not allowed	PLN 300	• Credit Card • Debit Card • **Effective through 12 April 2024** Electron Card	Must contain a PIN or CDCVM	N/A
Republic of Ireland	Not allowed	EUR 100	Debit Card	Must contain a PIN or CDCVM	N/A
Romania	Not allowed	RON 200	• Credit Card • Debit Card • **Effective**	Must contain a PIN or CDCVM	N/A

Table 5-16: Cash-Back Requirements (continued)

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
			through 12 April 2024 Electron Card		
Slovakia	Not allowed (must be in conjunction with a purchase of at least EUR 5)	EUR 50	• Credit Card • Debit Card • **Effective through 12 April 2024** Electron Card	Must contain a PIN or CDCVM	N/A
Sweden	Not allowed	SEK 2,000	• Credit Card • Debit Card	Must contain a PIN or CDCVM	N/A
Switzerland	Not allowed	**Effective through 12 June 2020** Between CHF 10 and CHF 200 **Effective 13 June 2020** Between CHF 20 and CHF 300	• Credit Card • Debit Card • Prepaid Card	Must contain a PIN or CDCVM	N/A
Turkey	Not allowed	Between TL 10 and TL 100	• **Effective through 12 April 2024** Electron Card • Direct (Immediate) Debit Card	Must contain a PIN or CDCVM	N/A
United Kingdom	**Effective**	GBP 100	• Debit Card	Must contain a	N/A

Table 5-16: Cash-Back Requirements (continued)

Region/Country	Cash-Back without Purchase	Cash-Back Amount Limits[1]	Allowed Product Types	Cardholder Verification	Other
	through 17 April 2020 Not allowed **Effective 18 April 2020** Allowed		• **Effective through 16 April 2021** Electron Card	PIN or CDCVM	
LAC Region					
Brazil	Not allowed	USD 200 (or local currency equivalent)	• Debit Card • Electron Card	Must contain a PIN or CDCVM	N/A
Costa Rica	Must be available	USD 250 (or local currency equivalent)	Debit Card	Must contain a PIN or CDCVM	N/A
Mexico	Not allowed	Between MXN 1,500 and MXN 2,000	Debit Card	Must contain a PIN or CDCVM	N/A
US Region					
US Region	Allowed	USD 200	• Debit Card • Prepaid Card	Must contain a PIN	Must participate in Partial Authorization
Other countries (only with Visa permission)					
[1] Merchants may set a lower Cash-Back Transaction amount limit at their discretion					

ID# 0002971   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.9.1.5   Processing of Quasi-Cash Transactions

For a Quasi-Cash Transaction, a Merchant must both:

- Process a Quasi-Cash Transaction as a purchase and not as a Cash Disbursement[1]

- In the US Region or a US Territory: Not add a service fee or commission to the Transaction if the Merchant assesses a US Credit Card Surcharge or Service Fee on the Transaction

[1] Except in the CEMEA Region (South Africa)

ID# 0002885	Edition: Apr 2020 | Last Updated: Oct 2018

5.9.1.6   Processing of the Sale of Travelers Cheques and Foreign Currency

A financial institution with authority to make Cash Disbursements that sells or disburses travelers cheques or foreign currency may process the Transaction as either a:

- Quasi-Cash Transaction

- Cash Disbursement

In the US Region: An Acquirer must not add to the Transaction amount any surcharge, commission, or fee.

ID# 0008694	Edition: Apr 2020 | Last Updated: Oct 2016

5.9.1.8   Wire Transfer Money Order Merchant Disclosures

A Wire Transfer Money Order Merchant that disburses checks or money orders must both:

- Advise the Cardholder that the Merchant accepting the Card is the wire transfer company, not the payee. The check or money order must be payable to the party cashing the check or money order.

- Disclose any fee to the Cardholder and include it on the Transaction Receipt

ID# 0002887	Edition: Apr 2020 | Last Updated: Oct 2015

5.9.1.9   Wire Transfer Money Order Requirements and Restrictions – US Region

In the US Region: Unless a Cardholder authorizes a Wire Transfer Money Order Merchant to process a Wire Transfer Money Order electronically, a Wire Transfer Money Order must be a written negotiable instrument that complies with all of the following:

- Is signed by the maker or drawer

- Is payable on demand

- Is payable to order or to bearer

Visa Product and Service Rules

- Unless otherwise specified, contains all of the following:
  - Federal Reserve routing symbol
  - Suffix of the institutional identifier of the paying bank or nonbank payor
  - Name, city, and state of the paying bank associated with the routing number

The Wire Transfer Money Order Merchant must comply with all of the following:

- In advertising and marketing materials associated with a money order purchase, both:
  - Specify that the Transaction involves the purchase of a money order
  - Clearly identify the Wire Transfer Money Order Merchant as the Merchant completing the Transaction
- Not use the Visa-Owned Marks to imply that a Cardholder may use a Card to either:
  - Pay for goods or services at the Merchant Outlet
  - Satisfy an outstanding Debt to the Merchant
- Disclose both of the following to the Cardholder in writing (or, for a telephone order, verbally):
  - The name of the Wire Transfer Money Order Merchant accepting the Card
  - That the Transaction is the purchase of a check or money order and that any subsequent Transaction with the third-party merchant is the same as a transaction made with cash
- Not include more than one Wire Transfer Money Order Transaction on a single check or money order
- Not complete a Wire Transfer Money Order Transaction if the funds are obtained to purchase goods or services at a third-party merchant outlet under the terms of the agreement between the Wire Transfer Money Order Merchant and third-party merchant. This does not apply to agreements involving any of the following:
  - Casino or other gambling establishment
  - Check-cashing outlet
  - Truck stop offering cash access services

ID# 0008440	Edition: Apr 2020	Last Updated: Apr 2020

5.9.1.10 Point-of-Sale Balance Inquiry and Point-of-Sale Balance Return Service – Acquirer Participation Requirements

An Acquirer that participates in the Point-of-Sale Balance Inquiry and/or a Point-of-Sale Balance Return Service must complete systems testing with Visa.

ID# 0025546   Edition: Apr 2020 | Last Updated: Oct 2018

5.9.1.14   Prepaid Card Compromise

A Merchant that sells Prepaid Cards must not sell a Prepaid Card if there is evidence of potential Card compromise, such as tampered packaging. The Merchant must retain the Card and follow recovered Card requirements.

ID# 0025787   Edition: Apr 2020 | Last Updated: Apr 2020

5.9.1.15   Mobile Push Payment Transactions – Cash-In and Cash-Out Requirements

A Merchant must not:

- Establish a minimum Cash-In or Cash-Out amount
- Process an international Cash-In Transaction
- Perform a Cash-In or Cash-Out Transaction in a currency other than the local currency
- Impose a fee on a Cash-In or Cash-Out Transaction

ID# 0030587   Edition: Apr 2020 | Last Updated: Oct 2018

5.9.1.16   Acquirer Use of Non-Reloadable Prepaid BIN and Account Range Data – Europe Region

In the Europe Region: If an Acquirer in the European Union chooses to receive a file from Visa containing data for BINs and Account Ranges that are used to issue Non-Reloadable Prepaid Cards, the Acquirer may use this data as part of their decision-making process when evaluating a Transaction, subject to both of the following:

- An Acquirer must use the data solely to comply with local laws and regulations
- An Acquirer must not share the data with Merchants or Third Party Agents

ID# 0030636   Edition: Apr 2020 | Last Updated: Oct 2019

5.9.2   Chip

5.9.2.1   Chip Transaction Acquirer Data Requirements

An Acquirer that processes a Chip-initiated Transaction must support Full-Chip Data processing via its host system and process VIS and Common Core Definitions Chip Cards.

ID# 0004842	Edition: Apr 2020	Last Updated: Apr 2018

5.9.2.2   Acquirer Liability for Fallback Transactions

Transactions accepted as Fallback Transactions are the liability of the Acquirer if both:

- The Card is a Chip Card containing a Visa and Visa Electron Smart Payment Application or an EMV and VIS-Compliant Plus application.
- Either:
  - Transaction is not authorized by the Issuer or the Issuer's agent
  - Transaction is authorized by the Issuer or the Issuer's agent, and the appropriate values identifying the Transaction as a Fallback Transaction are not included within the related Authorization Message

ID# 0001839	Edition: Apr 2020	Last Updated: Apr 2018

5.9.2.3   Global Chip Fallback Monitoring Program Criteria

An Acquirer that meets or exceeds all of the monthly performance activity levels for international[1] Chip-initiated Transactions will be placed in the Global Chip Fallback Monitoring Program.

Visa may both:

- Modify or create new monthly performance levels
- Apply the program to Domestic Transactions

[1] In the Europe Region: All Transactions that are Fallback Transactions are monitored as specified in *Section X*.

ID# 0008404	Edition: Apr 2020	Last Updated: Apr 2018

5.9.2.4   EMV Liability Shift – Acquirer Liability for Account Generated Counterfeit Fraud

An Acquirer is liable for counterfeit Transactions completed in a Card-Present Environment if all of the following:

- The Transaction did not take place at a Chip-Reading Device.
- The Account Number was not resident on the Issuer's master file on the Transaction Date.
- All valid Cards bearing Account Numbers within the same Account Range as the Counterfeit Card are Chip Cards containing a Visa or Visa Electron Smart Payment Application.

- The Transaction was below the Merchant's Floor Limit and did not receive Authorization.

- The Account Number was resident on the Exception File with a Pickup Response on the Processing Date of the Compliance filing and was on the Exception File for a total period of at least 30 calendar days from the date of listing.

ID# 0001819	Edition: Apr 2020	Last Updated: Oct 2019

5.9.2.5 EMV Liability Shift – Acquirer Liability for Card-Present Counterfeit Chip Card Transactions

Counterfeit Card Transactions completed in a Card-Present Environment are the liability of the Acquirer if both:

- The Card is a Chip Card containing a Visa or Visa Electron Smart Payment Application or an EMV and VIS-Compliant Plus application.

- Either:

  – The Transaction does not take place at a Chip-Reading Device and is not a Fallback Transaction completed following correct acceptance procedures.

  – The Transaction is Chip-initiated and the Acquirer does not transmit the Full-Chip Data to Visa.

The requirements in this section apply to qualifying Transactions, as specified in *Section 1.11.1.2, EMV Liability Shift Participation.*

This section does not apply if the Authorization record indicates that CVV verification was not performed or that the CVV failed verification.

For a Transaction not involving a Europe Member, this section does not apply if the Transaction contained a payment Token.

ID# 0001837	Edition: Apr 2020	Last Updated: Apr 2017

5.9.2.6 EMV Liability Shift – Acquirer Liability for Non-Counterfeit Card-Present Fraudulent Transactions

Non-Counterfeit Card fraudulent Transactions completed in a Card-Present Environment are the liability of the Acquirer if either:

- For a Chip-initiated Transaction without Online PIN, the Acquirer does not transmit the Full-Chip Data to Visa.

- All of the following:
  - The Transaction takes place at an Acceptance Device that is not EMV PIN-Compliant.
  - The Card is a PIN-Preferring Chip Card.
  - PIN Verification was not performed.

This section applies to qualifying Transactions, as specified in _Section 1.11.1.2, EMV Liability Shift Participation_.

ID# 0001838	Edition: Apr 2020 | Last Updated: Apr 2016

5.9.2.7   Acquirer Requirements for PIN Acceptance and Processing – AP Region (India)

In the AP Region (India): An Acquirer must comply with all of the following:

- Certify with Visa that its host system supports Chip data and the acceptance of EMV Chip Cards
- Only use or support an EMV-Compliant Acceptance Device with the chip functionality activated
- Deploy and activate PIN pads

ID# 0027956	Edition: Apr 2020 | Last Updated: Oct 2014

5.9.2.8   Acquirer Liability for Chip Transactions in Card-Present Environment – Canada Region

In the Canada Region: An Acquirer will be liable for a Transaction in a Card-Present Environment, whether or not the Transaction is Chip-initiated, when all of the following are true:

- Transaction does not take place at a Compliant Chip Card Reading Device with a PIN-entry device that supports plaintext and enciphered offline PIN at POS, or enciphered online PIN at ATMs
- Card is a Compliant Chip Card
- Transaction is reported as a fraudulent Transaction using one of the following fraud type codes:
  - 0 (lost)
  - 1 (stolen)
  - 2 (Card not received as issued [NRI])
  - 4 (Issuer-reported counterfeit)

- Account Number is listed on the Card Recovery Bulletin with an Exception File Pick-up of 04, 07, 41, or 43 on the Processing Date of the Dispute, and is on the Exception File for a total period of at least 60 calendar days from the date of listing

ID# 0004884	Edition: Apr 2020 | Last Updated: Apr 2018

5.9.2.10   Chip Transaction Processing Requirements – US Region

In the US Region: A transaction initiated with a Visa-owned Application Identifier must be processed as a Visa Transaction, a Visa Electron Transaction, an Interlink transaction, or a Plus transaction, as applicable.

This does not apply to transactions from US Covered Visa Debit Cards initiated with the Visa US Common Debit Application Identifier, a Plus-enabled ATM-only Proprietary Card, or an Interlink-enabled Proprietary Card.

ID# 0027580	Edition: Apr 2020 | Last Updated: Oct 2015

5.9.3   QR Code

5.9.3.1   QR Code Acquirer Data Requirements – AP Region

In an AP Region: An Acquirer that processes a QR code Transaction must support Full-Chip Data processing via its host system.

ID# 0029968	Edition: Apr 2020 | Last Updated: Apr 2020

5.9.4   Electronic Commerce

5.9.4.1   Merchant Website Requirements

An Electronic Commerce Merchant website and/or application must contain all of the following:

- Customer service contact, including email address or telephone number[1]
- Clearly and prominently display the country[2] of the Merchant Outlet[3], assigned as specified in *Section 1.5.1.2, Assignment of Merchant Outlet Location*,[3,4] or of the Marketplace, assigned as specified in *Section 5.3.2.1, Assignment of Payment Facilitator, Staged Digital Wallet Operator, or Marketplace Location,* either:
  - On the same screen view as the checkout screen used to present the final Transaction amount
  - Within the sequence of web pages that the Cardholder accesses during the checkout process

A link to a separate web page does not meet this requirement.[5]

- The address for Cardholder correspondence

- Policy for delivery of multiple shipments

- In addition, on an Online Gambling Merchant's homepage or payment page, all of the following:
    - The statement "Internet gambling may be illegal in the jurisdiction in which you are located; if so, you are not authorized to use your payment card to complete this transaction."
    - A statement of the Cardholder's responsibility to know the laws concerning online gambling in the Cardholder's country
    - A statement prohibiting the participation of individuals under a lawful age
    - A complete description of the rules of play, cancellation policies, and pay-out policies
    - A statement recommending that the Cardholder retain a copy of Transaction records and Merchant policies and rules
    - An Acquirer numeric identifier[6]

- In addition, in the Europe Region, the Merchant's consumer data privacy policy

In addition, a Marketplace must both:

- Disclose the country of the Marketplace retailer within the sequence of pages that the Cardholder accesses during the purchase process. A link to a separate web page does not meet this requirement.

- Make available to the Cardholder for at least 120 days from the Processing Date both:
    - The name of the retailer, Transaction Date, and Transaction amount
    - If the retailer is responsible for answering questions about the purchase of the goods, an easy means for the Cardholder to contact the retailer

[1] In the Europe Region: If the Merchant delivers goods or services outside of the Merchant Outlet country, both a local and an internationally accessible telephone number must be provided

[2] In the Europe Region: A Merchant or Sponsored Merchant must include the address of the Merchant Outlet.

[3] A travel agency acting on behalf of another Merchant must display the location of the travel agency. If travel or lodging is sold by a travel agency, the Transaction Country is the country in which the travel agency is located.

[4] In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Merchant or Sponsored Merchant that primarily operates from a personal residence is not required to provide the residence street address.

[5] In the Europe Region: This may be a link to another web page only if the link forms part of the "click to accept" acknowledgement and refers to the cancellation policy.

[6] Except in the Europe Region, specified by Visa.

ID# 0008635	Edition: Apr 2020 | Last Updated: Apr 2018

5.9.4.2   Electronic Commerce Payment Credential Security

An Electronic Commerce Merchant must not display the full Payment Credential to the Cardholder online.

ID# 0003627	Edition: Apr 2020 | Last Updated: Apr 2020

5.9.4.3   Acquirer Support of Visa Secure or Visa Checkout

An Acquirer must do all of the following:

- Notify its Electronic Commerce Merchant of the availability of Visa Secure

- Provide Visa Secure to its Electronic Commerce Merchant as requested

- Comply with *Table 5-17, Acquirer Support of Visa Secure by Region/Country/Territory – Requirements*

Table 5-17: Acquirer Support of Visa Secure by Region/Country/Territory – Requirements

Region/Country/Territory	Requirement
Australia	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: - MCC 4722 (Travel Agencies and Tour Operators) - MCC 4816 (Computer Network/Information Services) - MCC 4829 (Wire Transfer Money Orders) - MCC 5085 (Industrial Supplies) - MCC 5311 (Department Stores) - MCC 5399 (Miscellaneous General Merchandise) - MCC 5411 (Grocery Stores and Supermarkets) - MCC 5661 (Shoe Stores) - MCC 5691 (Men's and Women's Clothing Stores) - MCC 5699 (Miscellaneous Apparel and Accessory Shops) - MCC 5722 (Household Appliance Stores) - MCC 5732 (Electronics Stores)

Table 5-17: Acquirer Support of Visa Secure by Region/Country/Territory – Requirements (continued)

Region/Country/Territory	Requirement
	• MCC 5733 (Music Stores – Musical Instruments, Pianos, and Sheet Music)
	• MCC 5734 (Computer Software Stores)
	• MCC 5912 (Drug Stores and Pharmacies)
	• MCC 5943 (Stationery Stores, Office and School Supply Stores)
	• MCC 5944 (Jewelry Stores, Watches, Clocks, and Silverware Stores)
	• MCC 5999 (Miscellaneous and Specialty Retail Stores)
	• MCC 6211 (Security Brokers/Dealers)
	• MCC 7011 (Lodging – Hotels, Motels, Resorts, Central Reservation Services)
	• MCC 7832 (Motion Picture Theaters)
	• MCC 7995 (Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks)
	• MCC 8999 (Professional Services)
	• MCC 9402 (Postal Services – Government Only)
	If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 Cambodia	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls through Use of Magnetic Stripe Reading Telephones, and Fax Services) • MCC 8398 (Charitable Social Service Organizations) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 Hong Kong	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4722 (Travel Agencies and Tour Operators)

Table 5-17: Acquirer Support of Visa Secure by Region/Country/Territory – Requirements (continued)

Region/Country/Territory	Requirement
	• MCC 4812 (Telecommunication Equipment and Telephone Sales) • MCC 5045 (Computers and Computer Peripheral Equipment and Software) • MCC 5621 (Women's Ready-To-Wear Stores) • MCC 5691 (Men's and Women's Clothing Stores) • MCC 5732 (Electronics Stores) • MCC 5734 (Computer Software Stores) • MCC 5816 (Digital Goods – Games) • MCC 5945 (Hobby, Toy, and Game Shops) • MCC 5999 (Miscellaneous and Specialty Retail Stores) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
India	• Ensure that its Electronic Commerce Merchant processes Electronic Commerce Transactions using Visa Secure or Visa Checkout[2] • Not process a domestic Electronic Commerce Transaction unless the Cardholder has been successfully authenticated using Visa Secure or Visa Checkout[2]
Effective 18 April 2020 Indonesia	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5999 (Miscellaneous and Specialty Retail Stores) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 Macau	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4722 (Travel Agencies and Tour Operators)

Table 5-17: Acquirer Support of Visa Secure by Region/Country/Territory – Requirements (continued)

Region/Country/Territory	Requirement
	• MCC 4812 (Telecommunication Equipment and Telephone Sales)
	• MCC 5045 (Computers and Computer Peripheral Equipment and Software)
	• MCC 5621 (Women's Ready-To-Wear Stores)
	• MCC 5691 (Men's and Women's Clothing Stores)
	• MCC 5732 (Electronics Stores)
	• MCC 5734 (Computer Software Stores)
	• MCC 5816 (Digital Goods – Games)
	• MCC 5945 (Hobby, Toy, and Game Shops)
	• MCC 5999 (Miscellaneous and Specialty Retail Stores)
	If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 Malaysia	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs:
	• MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified])
	• MCC 5977 (Cosmetic Stores)
	• MCC 5999 (Miscellaneous and Specialty Retail Stores)
	• MCC 7011 (Lodging – Hotels, Motels, Resorts, Central Reservation Services)
	If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
New Zealand	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs:
	• MCC 4722 (Travel Agencies and Tour Operators)
	• MCC 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls through Use of Magnetic Stripe Reading Telephones, and Fax Services)

Table 5-17: Acquirer Support of Visa Secure by Region/Country/Territory – Requirements (continued)

Region/Country/Territory	Requirement
	• MCC 5045 (Computers and Computer Peripheral Equipment and Software) • MCC 5310 (Discount Stores) • MCC 5722 (Household Appliance Stores) • MCC 5732 (Electronics Stores) • MCC 5734 (Computer Software Stores) • MCC 5941 (Sporting Goods Stores) • MCC 9402 (Postal Services – Government Only) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 Philippines	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 3000-3350 (Airlines, Air Carriers) • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls through Use of Magnetic Stripe Reading Telephones, and Fax Services) • MCC 4900 (Utilities – Electric, Gas, Water, and Sanitary) • MCC 5045 (Computers and Computer Peripheral Equipment and Software) • MCC 5331 (Variety Stores) • MCC 5399 (Miscellaneous General Merchandise) • MCC 5499 (Miscellaneous Food Stores – Convenience Stores and Specialty Markets) • MCC 5722 (Household Appliance Stores) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.

Table 5-17: Acquirer Support of Visa Secure by Region/Country/Territory – Requirements (continued)

Region/Country/Territory	Requirement
Effective 18 April 2020 Singapore	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5815 (Digital Goods Media – Books, Movies, Music) • MCC 5816 (Digital Goods – Games) • MCC 5817 (Digital Goods – Applications [Excludes Games]) • MCC 5818 (Digital Goods – Large Digital Goods Merchant) • MCC 5968 (Direct Marketing – Continuity/Subscription Merchant) • MCC 8999 (Professional Services) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 South Korea	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 5968 (Direct Marketing – Continuity/Subscription Merchant) • MCC 5999 (Miscellaneous and Specialty Retail Stores) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 16 January 2021 Taiwan	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4112 (Passenger Railways) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 7372 (Computer Programming, Data Processing, and Integrated Systems Design Services)

Table 5-17: Acquirer Support of Visa Secure by Region/Country/Territory – Requirements (continued)

Region/Country/Territory	Requirement
	If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 Thailand	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5968 (Direct Marketing – Continuity/Subscription Merchant) • MCC 8999 (Professional Services) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
Effective 18 April 2020 Vietnam	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,[1] if it is assigned any of the following MCCs: • MCC 4511 (Airlines and Air Carriers [Not Elsewhere Classified]) • MCC 4722 (Travel Agencies and Tour Operators) • MCC 5311 (Department Stores) • MCC 7994 (Video Game Arcades/Establishments) If a Merchant is not enrolled in Visa Secure with 3-D Secure 2.0 and is identified by the Visa Fraud Monitoring Program, it will be subject to the High Risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
CEMEA Region	Process Electronic Commerce Transactions using Visa Secure
Nigeria	Not process a domestic Electronic Commerce Transaction unless the Cardholder has been successfully authenticated using Visa Secure
Europe Region	Process Secure Electronic Commerce Transactions using Visa Secure

[1] A Merchant must adhere to an Issuer's requested authentication method.

[2] This applies only to Visa Checkout Transactions less than or equal to INR 2,000.

5.9.4.4   Visa Secure Dispute Protection Limitations – US Region

In the US Region: An Acquirer must notify its Visa Secure Merchant that its Electronic Commerce Transactions are not eligible for Dispute protection from Dispute Condition 10.4: Other Fraud – Card-Absent Environment if either:

- The Merchant is classified with one of the following MCCs:
  - MCC 4829 (Wire Transfer Money Orders)
  - MCC 5967 (Direct Marketing – Inbound Teleservices Merchant)
  - MCC 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [not Money Transfer], Travelers Cheques, and Debt Repayment)
  - MCC 6540 (Non-Financial Institutions: Stored Value Card Purchase/Load)
  - MCC 7801 (Government Licensed On-Line Casinos [On-Line Gambling])
  - MCC 7802 (Government-Licensed Horse/Dog Racing)
  - MCC 7995 (Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks)
- The Merchant has been identified in the Visa Fraud Monitoring Program. The Acquirer must notify the Merchant that it remains ineligible while it is in the program. This condition also applies if the Merchant enabled Visa Secure while identified in the program.

5.9.5   Visa Digital Commerce

5.9.5.1   Visa Digital Commerce Program (VDCP) Acquirer Participation Requirements

Effective 18 April 2020 An Acquirer that either itself, or through its agents/subsidiaries, participates in the Visa Digital Commerce Program (VDCP) must do all of the following:

- Comply, and ensure that its agents/subsidiaries comply, with the Visa Rules and the Visa Digital Commerce Program Documentation, which include but are not limited to technical, registration, testing, approval, certification, and privacy and security requirements
- Obtain written confirmation from Visa that it has met such requirements before releasing any VDCP-related products or services

- If notified by Visa (which may include via email or telephone), or otherwise made aware of the Acquirer's or its agent's non-compliance with the VDCP requirements specified in the Visa Rules or the Visa Digital Commerce Program Documentation, take prompt action to remedy the non-compliant situation

Visa reserves the right to suspend or terminate an Acquirer's or its agent's participation in the program, in whole or in part, if Visa reasonably believes that such participation could cause harm to the program or related intellectual property rights, including for security incidents and non-compliance with applicable law.

ID# 0030683	Edition: Apr 2020 | Last Updated: New

5.9.5.2   Acquirer's Use of Issuer's Pass-Through Digital Card Art

An Acquirer that receives pass-through rights from Visa to use, reproduce, and display Issuer trademarks, service marks, logos, and Issuer-provided digital Card art (collectively, for purposes of this rule, Issuer intellectual property) in connection with the Acquirer's participation in the Visa Digital Commerce Program (VDCP) must not alter such Issuer intellectual property or the metadata in any unauthorized way. The Acquirer must ensure that its affiliates/designees do not alter or cause the Issuer intellectual property or metadata to be altered in any unauthorized way.

ID# 0030684	Edition: Apr 2020 | Last Updated: New

5.9.5.3   License Grant for the Visa Digital Commerce Program (VDCP)

Subject to an Acquirer and its agents/subsidiaries' compliance with the Visa Rules and the Visa Digital Commerce Program Documentation, Visa grants to an Acquirer and its agents/subsidiaries participating in the Visa Digital Commerce Program (VDCP) a royalty-free, non-exclusive, revocable, non-transferable (unless stated otherwise), non-sublicensable license to:

- Use the operational and technical documentation, branding guidelines, software development kits, uniform resource identifiers, public encryption keys, and other tools provided by Visa or its affiliates in connection with the program
- Modify the sample source code relating to the program
- Make a reasonable number of back-up or test copies of the materials provided under the program

An Acquirer's or its agents/subsidiaries' use of the VDCP materials is limited solely to the extent necessary to enable its participation in any part of the VDCP in compliance with the Visa Rules and the Visa Digital Commerce Program Documentation.

The VDCP materials are licensed and not sold. Visa reserves all rights not expressly granted by the VDCP license.

ID# 0030685   Edition: Apr 2020 | Last Updated: New

5.9.6   Mail/Phone Order Transactions

5.9.6.1   Disclosure of Mail/Phone Order Merchant Outlet Country

A Mail/Phone Order Merchant must disclose the Merchant Outlet country when presenting payment options to a Cardholder.

ID# 0002902   Edition: Apr 2020 | Last Updated: Oct 2014

5.9.7   Aggregated Transactions

5.9.7.1   Aggregated Transaction Merchant Requirements

Only the following Merchants may process an Aggregated Transaction:

- Electronic Commerce Merchants
- Merchants assigned one of the following MCCs:
    - 4111 (Local and Suburban Commuter Passenger Transportation, Including Ferries)
    - 4112 (Passenger Railways)
    - 4131 (Bus Lines)

An Aggregated Transaction must comply with all of the following:

- In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: Not include purchases made more than 7 calendar days apart
- In the US Region: Not include purchases made more than 3 calendar days apart
- For an Electronic Commerce Transaction, not exceed USD 15 (or local currency equivalent)
- For a Transaction (excluding a Mass Transit Transaction) with MCC 4111, 4112, or 4131, not exceed:
    - In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: USD 25 (or local currency equivalent)
    - In the US Region: USD 15

For an Aggregated Transaction, a Merchant must do all of the following:

- At the Point of Transaction, inform the Cardholder of all of the following:
  – That Transaction aggregation will occur
  – The Transaction aggregation terms, including the maximum number of calendar days and Transaction value
  – How to obtain details of the aggregated purchases
- Make individual purchase information and Aggregated Transaction information available to a Cardholder for at least 120 days after the processing date of the Aggregated Transaction
- In the US Region: Both:
  – Be able to process a Partial Authorization
  – For an Electronic Commerce Transaction, obtain an Authorization of no more than USD 15 at the start of each aggregation session

ID# 0002906	Edition: Apr 2020 | Last Updated: Oct 2019

5.9.8   T&E and Rental Transactions

5.9.8.1   Acquirer Requirements for Airlines

When entering into a Merchant Agreement with an Airline for Airline ticket sales, an Acquirer must do all of the following:

- Meet Visa capitalization and reserve requirements
- Submit to Visa, for Visa's approval, a business plan setting out the expected Transaction volumes and applicable risk reduction measures, in advance of submitting Transactions on behalf of either:
  – A newly acquired Airline
  – A currently acquired Airline, where that Airline is providing services in a new country or has adopted an alternative payment channel

ID# 0030631	Edition: Apr 2020 | Last Updated: Apr 2019

5.9.8.2   Merchant Requirements for Guaranteed Reservations

If a Merchant accepts a Guaranteed Reservation, the Merchant must do all of the following:

- Be one of the following Merchant types:
  - – Lodging Merchant
  - – Aircraft rental Merchant
  - – Bicycle rental Merchant
  - – Boat rental Merchant
  - – Equipment rental Merchant
  - – Motor home rental Merchant
  - – Motorcycle rental Merchant
  - – Trailer park or campground
  - – Vehicle Rental Merchant
- Provide disclosure of reservation conditions to the Cardholder at the time of the reservation. If the reservation was made by telephone, the Merchant must send to the Cardholder a written reservation confirmation containing all required disclosures within 24 hours of the reservation.
- Provide to the Cardholder a period of at least 24 hours after delivery of the reservation confirmation to cancel the reservation without penalty
- Hold the reservation for at least 24 hours after the agreed start time unless the Cardholder cancels the reservation by the time specified in the Merchant's cancellation policy
- If the Cardholder claims the reservation within 24 hours of the agreed start time, and the Merchant has failed to hold the reservation, provide at no cost to the Cardholder comparable accommodation, merchandise, or services, and pay for associated costs, or as otherwise agreed by the Cardholder, until the reserved accommodation, merchandise, or services become available
- Process a No-Show Transaction only if the Cardholder has not properly cancelled the reservation according to the disclosed and agreed cancellation policy and has not claimed the reservation

ID# 0029266   **Edition: Apr 2020 | Last Updated: Apr 2018**

5.9.8.3   Conditions for Assessing Amended Amounts or Delayed Charges

A Merchant may process a Transaction evidencing an amended amount or delayed charge, only as follows:

Table 5-18: Conditions for Amended Amounts and Delayed Charges

	Amended Amounts	Delayed Charges for Loss, Theft, or Damage[1]	All Other Delayed Charges
Eligible Merchant types	• Aircraft rental Merchant • Bicycle rental Merchant • Boat rental Merchant • Cruise Line • Equipment rental Merchant • Lodging Merchant • Motor home rental Merchant • Motorcycle rental Merchant • Trailer parks and campgrounds • Vehicle Rental Merchant		
The charge must:	Be directly related to both: • The merchandise or services provided by the Merchant to the Cardholder (for example: insurance or rental fees) • A Transaction in which the Cardholder participated	Comply with all of the following: • Be directly related to the merchandise or services provided by the Merchant to the Cardholder during the rental period • Be the actual cost for replacement/repair of damage to the Merchant's property or for an insurance deductible, whichever is less • If an Advance Payment, not be used to pay for damage, theft, or loss of use	Be directly related to both: • The merchandise or services provided by the Merchant to the Cardholder (for example: tolls or parking tickets) • A Transaction in which the Cardholder participated
To support the charge, the Merchant	The amended Transaction Receipt	Within 10 business days of	Both:

Table 5-18: Conditions for Amended Amounts and Delayed Charges (continued)

	Amended Amounts	**Delayed Charges for Loss, Theft, or Damage[1]**	**All Other Delayed Charges**
must provide to the Cardholder:		the rental return, check-out, or disembarkation date, and before processing any additional Transaction, documentation that does all of the following: - Explains the charge and connects the charge to the Cardholder's use of the merchandise or services during the rental period - Includes[2] any accident, police, or insurance report - For damage to a rental vehicle, provides at least 2 quotes from entities that are legally permitted to perform repairs - Specifies the portion of the loss, theft, or damage that will be paid by insurance and the reason that the Cardholder is liable for the amount claimed - Informs the Cardholder that payment for loss, theft, or damage with the Cardholder's Visa Card is optional and not a required or default	- The Transaction Receipt for the delayed charge - An explanation of the charge (if for a parking ticket or traffic violation, this must include documentation from the appropriate civil authority with the license number of the rental vehicle, the time and location of the violation, and the amount of the penalty in the currency of the civil authority)

Table 5-18: Conditions for Amended Amounts and Delayed Charges (continued)

	Amended Amounts	Delayed Charges for Loss, Theft, or Damage[1]	All Other Delayed Charges
		payment option	
The Cardholder must expressly approve the charge before the Merchant processes the Transaction (except in the Europe Region):	No, unless required by applicable laws or regulations	In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Yes. The Cardholder must expressly agree in writing to pay the specific charges after the loss, theft, or damage has occurred and after receiving all required disclosures and amounts from the Merchant. In the Europe Region: • The Cardholder may, within 10 business days of receiving this confirmation, and at no cost to the Merchant, provide an alternative written estimate for the cost of repairing the damage. • If agreement is not reached between the Merchant and the Cardholder for the cost of repairing the damage, and if the Merchant processes the delayed charge Transaction, the Cardholder may dispute the Transaction. • The Merchant must wait	No

Table 5-18: Conditions for Amended Amounts and Delayed Charges (continued)

	Amended Amounts	Delayed Charges for Loss, Theft, or Damage[1]	All Other Delayed Charges
		20 business days from the date of the confirmation receipt provided to the Cardholder before processing a delayed charge for damages.	
The Merchant must process the charge within:	24 hours of check-out or rental return	90 calendar days of the rental return, check-out, or disembarkation date	
[1] Requirements for rental Merchants in the Europe Region are specified in *Section 5.9.8.4, Rental Merchant Charges for Damages – Europe Region*			
[2] Required for Transactions involving car or truck rental. For all other Merchants, as applicable			

ID# 0007398	Edition: Apr 2020	Last Updated: Apr 2020

5.9.8.4   Rental Merchant Charges for Damages – Europe Region

In the Europe Region: When a rental Merchant carries out a delayed charge Transaction for charges relating to damage to a rental vehicle, the Merchant must provide the Acquirer with all of the following:

- A copy of the rental agreement

- An estimate of the cost of the damage from an organization that can legally provide repairs

- The relevant civil authority's accident report (if applicable)

- Documentation showing that the Cardholder has given consent that a delayed charge Transaction may be processed using the Cardholder's Card to cover damages to a rental vehicle. This consent must be evidenced by either:

  – The Cardholder's signature on the same page as, and close to, the description of the charges that may be covered by the delayed charge Transaction

  – The Cardholder's signature on the agreement and the Cardholder's initials on each page of the agreement, including on the same page as the description of the charges that may be covered by the delayed charge Transaction

- Any other documentation demonstrating the Cardholder's liability for the damage

- A copy of the insurance policy of the rental Merchant, if the Merchant requires that the Cardholder pay an insurance deductible for damages and a copy of the vehicle rental agreement showing that the Cardholder consents to be responsible for the insurance deductible

ID# 0004141	Edition: Apr 2020	Last Updated: Apr 2017

5.9.9   Dynamic Currency Conversion

5.9.9.1   Dynamic Currency Conversion (DCC) – Acquirer Requirements

Before processing a Dynamic Currency Conversion (DCC) Transaction, an Acquirer must both:

- Comply with the DCC registration and certification requirements specified in the *DCC Guide*

- Ensure that each Merchant Outlet or ATM that conducts DCC both:

  – Complies with the Visa Rules and the *DCC Guide*

  – Does not offer DCC on consumer Prepaid Cards or consumer Debit Cards enabled with the Visa Multi-Currency Solution, or on consumer travel Prepaid Cards (including Visa TravelMoney)[1]

[1] See the *DCC Guide* for information on the account billing currency file to identify applicable Account Ranges.

ID# 0025740	Edition: Apr 2020	Last Updated: Apr 2020

5.9.9.3   Dynamic Currency Conversion (DCC) – Merchant and ATM Requirements

A Merchant or ATM Acquirer that offers Dynamic Currency Conversion (DCC) must comply with all of the following:

- Inform the Cardholder that DCC is optional and not use any language or procedures that may cause the Cardholder to choose DCC by default

- Ensure that the Cardholder is given all the relevant information to allow them to make a clear and transparent decision to expressly agree[1] to a DCC Transaction

- Not misrepresent, either explicitly or implicitly, that its DCC service is a Visa service[2]

- Offer DCC in the Cardholder Billing Currency

- Not impose any additional requirements on the Cardholder to have the Transaction processed in the local currency

Visa Product and Service Rules

5 Acceptance

Visa Core Rules and Visa Product and Service Rules

- Not convert a Transaction amount in the local currency that has been approved by the Cardholder into an amount in the Cardholder Billing Currency after the Transaction has been completed but not yet entered into Interchange

- In the US Region or a US Territory: Include the US Credit Card Surcharge amount, if assessed, in the conversion

- In the AP Region (Australia): Include any Surcharge amount, if assessed, in the conversion

If an Electronic Commerce Merchant uses a Cardholder's Payment Credential to determine eligibility to convert the purchase amount from the Merchant's currency to the Cardholder Billing Currency it must comply with all requirements relating to a DCC Transaction.

[1] A Cardholder must actively make a selection (for example: checking a box or button) and the DCC option must not be pre-selected.

[2] In the Europe Region: Inform the Cardholder before obtaining Authorization that DCC is a service provided by the Merchant or Acquirer

---

ID# 0003100	Edition: Apr 2020 | Last Updated: Apr 2020

5.9.10   Advance Payments and Repeated Payments

5.9.10.1   Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials

Effective through 24 January 2020 A Merchant or its agent, a Payment Facilitator, or a Digital Wallet Operator that processes partial and full prepayments and that stores a Stored Credential and/or processes Transactions using a Stored Credential must comply with *Table 5-19, Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020).*

These requirements do not apply to the following when the Merchant or its agent uses the Stored Credential for a single Transaction or a single purchase:

- A No-Show Transaction

- A Transaction involving an amended amount or a delayed charge

- A Transaction involving an Incremental Authorization

- A Transaction where the Merchant is allowed to submit a new Authorization Request for the same Transaction

- A Transaction that received a Decline Response and is resubmitted for Authorization, as specified in *Section 7.3.6.1, Preauthorized Transaction Decline Response*

Table 5-19: Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020)

Prepayment (Partial)	Prepayment (Full)	Transaction Using a Stored Credential
Eligible Purchases		
Any	Any of the following: • T&E • Custom merchandise or services • In a Face-to-Face Environment, where not all items purchased in the Transaction are immediately available but will be shipped or provided at a later date • Recreational services or activities related to tourism and travel	Any
Disclosure to Cardholder and Cardholder Consent		
When entering into a Cardholder agreement, all requirements related to the specific Transaction type listed below must be clearly displayed at the time that the Cardholder gives their consent and must be displayed separately from the general purchase terms and conditions.		
The Merchant must provide, and the Cardholder must consent to,[1] all of the following in writing at the time of the first or only partial prepayment: • Description of promised merchandise or services • Terms of service	The Merchant must provide, and the Cardholder must consent to,[1] all of the following in writing at the time of the full prepayment: • Description of promised merchandise or services • Terms of service	When capturing a Stored Credential for the first time, the Merchant or its agent, the Payment Facilitator, or the Staged Digital Wallet Operator must establish an agreement with the Cardholder[1] that contains all of the following: • A truncated version of the Stored Credential (for example: last 4 digits of the Account Number), as it may be updated from time to time • How the Cardholder will be notified of any changes to the agreement

Table 5-19: Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020) (continued)

Prepayment (Partial)	Prepayment (Full)	Transaction Using a Stored Credential

• Timing of delivery to Cardholder
 	
• Transaction amount
 	
• Total purchase price
 	
• Terms of final payment, including the amount and currency
 	
• Cancellation and refund policies
 	
• Date and time that any cancellation privileges expire without prepayment forfeiture
 	
• Any associated charges
	• Timing of delivery to Cardholder
	
	• Transaction amount
	
	• Refund policies
	
	• Date and time that any refund privileges expire without prepayment forfeiture
	
	• Any associated charges
		• How the Stored Credential will be used
		
		• The expiration date of the agreement, if applicable
		
		• **Effective 18 April 2020** The length of any trial period, introductory offer, or promotional period
		
		In the Europe Region: The Merchant must provide the Cardholder with confirmation of the establishment of the Recurring Transaction agreement within 2 business days.
		
		In addition, before processing an Installment Transaction, Recurring Transaction, or Unscheduled Credential-on-File Transaction, the Merchant or its agent must obtain the Cardholder's express informed consent[1] to an agreement that contains all of the following:
		
		• The Transaction amount (including all associated taxes and charges) or a description of how the Transaction amount will be determined
		
		• The Transaction currency
		
		• Where surcharging is permitted, acknowledgement of any surcharge assessed and the associated disclosures
		
		• Cancellation and refund policies
		
		• The location of the Merchant Outlet
		
		• In addition, for Installment Transactions, both:
		
		  – Total purchase price
		
		  – Terms of future payments, including the dates, amounts, and currency
		
		• In addition, for Recurring Transactions, the Merchant must both:
		
		  – Include the fixed dates or intervals on which the Transactions will be processed

Table 5-19: Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020) (continued)

Prepayment (Partial)	Prepayment (Full)	Transaction Using a Stored Credential

		– At least 7 days before a Recurring Transaction, notify the Cardholder via email or other agreed method of communication if any of the following:
		
		▪ **Effective 18 April 2020** A trial period, introductory offer, or promotional period is going to end. The Merchant must include in the communication the Transaction amount and Transaction Date of subsequent Recurring Transactions and a link or other simple mechanism to enable the Cardholder to easily cancel Transactions online or via SMS/text message.
		
		▪ In the Europe Region:
		
		  ▪ More than 6 months have elapsed since the previous Recurring Transaction.
		
		  ▪ The Recurring Transaction agreement has been changed, including the amount of the Recurring Transaction, the date of the Recurring Transaction, or any other terms of the agreement.
		
		  ▪ **Effective through 17 April 2020** A trial period, introductory offer, or promotional period is going to end. The Merchant must include in the communication the Transaction amount and Transaction Date of subsequent Recurring Transactions and a link or other simple mechanism to enable the Cardholder to easily cancel Transactions online or via SMS/text message.
		
		● In addition, for Unscheduled Credential-on-File Transactions:
		
		– The agreement must include the event that will

Table 5-19: Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020) (continued)

Prepayment (Partial)	Prepayment (Full)	Transaction Using a Stored Credential
		prompt the Transaction (for example: if the Cardholder's balance falls below a certain amount). – In the Europe Region: The Merchant must provide notification to the Cardholder of any change in the Transaction amount or any other terms of the agreement at least 2 working days before the change. The Merchant or its agent, the Payment Facilitator, or the Staged Digital Wallet Operator must retain the Cardholder's agreement for the duration of the agreement and provide it to the Issuer upon request.
Amount		
A prepayment amount must be less than the cost of the merchandise or services purchased and must be applied to the total obligation.	The prepayment amount must be equal to the cost of the merchandise or services purchased.	The amount: • For an Installment Transaction, may include interest charges, except in the US Region • For a Recurring Transaction or an Unscheduled Credential-on-File Transaction, must not include finance charges
Transaction Processing Requirements		
Online Authorization for each Transaction.[2] The amount authorized must be no more than the amount of the individual Transaction. If an Authorization Request for a subsequent payment is declined, the Merchant must notify the Cardholder in writing and allow the Cardholder at	The Merchant must comply with all requirements applicable to the Transaction type.	Online Authorization for the initial and subsequent Transactions. The amount authorized must be no more than the amount of the individual Transaction. When capturing a Stored Credential for the first time, the Merchant or its agent, the Payment Facilitator, or the Staged Digital Wallet Operator must do all of the following: • Either: – Submit an Authorization Request for the amount due – If payment is not required, submit an Account

Table 5-19: Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020) (continued)

Prepayment (Partial)	Prepayment (Full)	Transaction Using a Stored Credential

least 7 days to pay by other means.		Verification
		
		• Use the appropriate indicator in the POS environment field
		
		• If the initial Authorization Request or Account Verification is not approved, not store the credential
		
		For a Transaction using a Stored Credential, the Merchant or its agent, the Payment Facilitator, or the Staged Digital Wallet Operator must use POS Entry Mode code 10.
		
		In addition, for a subsequent Recurring Transaction, Installment Transaction, or Unscheduled Credential on File Transaction, the Merchant or its agent, the Payment Facilitator, or the Staged Digital Wallet Operator must use the appropriate indicator in the POS environment field.[2]
		
		For a Transaction using a Stored Credential initiated by the Cardholder, the Merchant or its agent must also validate the Cardholder's identity (for example: with a login ID and password) before processing each Transaction.
		
		For an Installment Transaction, all of the following:
		
		• If an Authorization Request for a subsequent payment is declined, the Merchant or its agent must notify the Cardholder in writing and allow the Cardholder at least 7 days to pay by other means.
		
		• A Merchant or its agent must not process an initial Installment Transaction until the merchandise or services have been provided to the Cardholder and must not process individual Installment Transactions at intervals less than either:
		
		  – 7 calendar days
		
		  – In the US Region: The monthly anniversary of

Table 5-19: Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020) (continued)

Prepayment (Partial)	Prepayment (Full)	Transaction Using a Stored Credential
		the shipment date • Except as specified in the *Visa International Certificate of Incorporation and By-Laws,* Visa assumes no liability for an Installment Transaction processed more than 30 calendar days from the Authorization date.
Cancellation Procedure		

If the Cardholder cancels within the terms of the cancellation policy, the Merchant must provide to the Cardholder both of the following within 3 business days:
 	
• Cancellation or refund confirmation in writing
 	
• Credit Transaction Receipt for the amount specified in the cancellation policy
	If the Cardholder cancels within the terms of the cancellation policy, the Merchant must provide to the Cardholder both of the following within 3 business days:
	
	• Cancellation or refund confirmation in writing
	
	• Credit Transaction Receipt for the amount specified in the cancellation policy
		The Merchant or its agent must both:
		
		• Provide a simple cancellation procedure, and, if the Cardholder's order was initially accepted online, at least an online cancellation procedure
		
		• Not complete a Transaction:
		
		  – Beyond the duration expressly agreed by the Cardholder
		
		  – If the Cardholder requests that the Merchant or its agent change the payment method
		
		  – If the Cardholder cancels according to the agreed cancellation policy
		
		  – If it receives a Decline Response
		
		For an Installment Transaction, if the Cardholder cancels within the terms of the cancellation policy, the Merchant or its agent must provide to the Cardholder both of the following within 3 business days:
		
		• Cancellation or refund confirmation in writing
		
		• Credit Transaction Receipt for the amount specified in the cancellation policy

Retention of Payment		
If the Cardholder does	If the Cardholder does not cancel within the	None

Table 5-19: Requirements for Prepayments and Transactions Using Stored Credentials (Effective through 24 January 2020) (continued)

Prepayment (Partial)	Prepayment (Full)	Transaction Using a Stored Credential
not pay the balance and does not cancel within the terms of the cancellation policy, the Merchant may retain a partial prepayment only if the Merchant has disclosed on the Transaction Receipt that the prepayment is nonrefundable.	terms of the cancellation policy, the Merchant may retain a full prepayment only if the Merchant has disclosed on the Transaction Receipt that the prepayment is nonrefundable.	
Merchant Responsibility to Refund an Amount and Provide a Comparable Substitute		
The Merchant must refund the full amount paid if the Merchant has not adhered to the terms of the sale or service. If the Cardholder claims a reservation, and the Merchant has not held the reservation, the Merchant must provide at no additional cost to the Cardholder comparable merchandise or services and pay any associated costs for the remainder of the reserved time period, or as agreed between the Merchant and the Cardholder.		The Merchant or its agent must refund the full amount paid if the Merchant has not adhered to the terms of the sale or service.

[1] Where required by applicable laws or regulations, the Merchant or its agent must also provide to the Cardholder a record of the Cardholder's consent.

[2] In the LAC Region (Brazil): This does not apply to a domestic Installment Transaction.

Effective 25 January 2020 A Merchant or its agent that processes Partial Payments, Advance Payments, and Transactions using a Stored Credential must comply with *Table 5-20, General Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials (Effective 25 January 2020)* and as applicable, *Table 5-21, Transaction-Specific Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials (Effective 25 January 2020)*.

These requirements do not apply to the following when the Merchant or its agent uses the Stored Credential for a single Transaction or a single purchase:

- A No-Show Transaction

- A Transaction involving an amended amount or a delayed charge

- A Transaction involving an Incremental Authorization

- A Transaction where the Merchant is allowed to submit a new Authorization Request for the same Transaction

- A Transaction that received a Decline Response and is resubmitted for Authorization, as specified in *Section 7.3.6.1, Preauthorized Transaction Decline Response*

Table 5-20: General Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials (Effective 25 January 2020)

Requirement	Description

Disclosure and Agreement	Before a Merchant either stores a credential for a future Transaction or completes an Advance Payment, or Partial Payment, the Merchant must obtain the Cardholder's express informed consent to an agreement that contains all of the following:
	
	- Information related to the purchase, including:
	  – Description of goods or services
	  – Total purchase price
	  – Cancellation and refund policies, including the date that any cancellation privileges expire without Advance Payment forfeiture
	  – Where surcharging is permitted, acknowledgment of any surcharge assessed and the associated disclosures
	- Information about the Merchant, including:
	  – The location of the Merchant Outlet
	  – Address, email address, and phone number to use to contact the Merchant in relation to the Transactions
	- Terms and conditions related to the Stored Credential and future Transactions (where applicable), including:
	  – The Account Number that will be used to make payment (last four digits only), as it may be updated from time to time
	  – How the Cardholder will be notified of any changes to the agreement
	  – Transaction amount or a description of how the Transaction amount will be determined

Table 5-20: General Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials (Effective 25 January 2020) (continued)

Requirement	Description
	– The Transaction Currency
	– How the Stored Credential will be used
	– Timing and frequency of Transactions (does not apply if the Stored Credential will be used for Unscheduled Credential-on-File Transactions).
	– If the Stored Credential will be used for Unscheduled Credential-on-File Transactions, the event that will prompt the Transaction (for example: if the Cardholder's balance falls below a certain amount)
	– The expiration date of the agreement, if applicable
	– **Effective 18 April 2020** The length of any trial period, introductory offer, or promotional period
	When entering into a Cardholder agreement, all requirements related to these specific Transaction types must be clearly displayed at the time that the Cardholder gives their consent and must be displayed separately from the general purchase terms and conditions.
	In the Europe Region: The Merchant must provide the Cardholder with confirmation of the establishment of the Recurring Transaction agreement within 2 business days.
	In the Europe Region: For Unscheduled Credential-on-File Transactions, the Merchant must provide notification to the Cardholder of any change in the Transaction amount or any other terms of the agreement at least 2 working days before the change.
	The Merchant must retain this information for the duration of the agreement and provide it to the Cardholder or Issuer upon written request.
Amount	A Recurring Transaction or an Unscheduled Credential-on-File, Transaction must not include any finance charges, interest, or imputed interest.
Refund	The Merchant must refund the full amount paid if the Merchant has not adhered to the terms and conditions of the sale or service.

Table 5-21: Transaction-Specific Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials (Effective 25 January 2020)

Transaction Type	Requirement

Partial Payment	An Acquirer must ensure that for a Partial Payment, the Merchant does not charge any interest, or imputed interest, to the Cardholder. If the Merchant applies a late payment fee, it must be a flat fee and must be applied only as a late payment penalty.
	
	 Additionally, for a Partial Payment where the Merchant is not the seller of the goods or services being purchased, the Merchant (or its affiliate) must have a direct contract with the seller and comply with all of the following:
	
	 • Be located in the same country[1] as the seller of the goods or services
	
	 • For each new Partial Payment agreement, disclose to the Cardholder that:
	   – It is not the seller of the goods or services and disclose the name of the actual seller
	   – Disputes for non-delivery and quality of goods or services will not be available in relation to the goods or services purchased
	   – The Cardholder's Issuer may charge interest, or other charges, in line with the terms and conditions of the agreement between the Cardholder and the Issuer
	
	 • Not state or imply that interest will not be charged by the Issuer for the Partial Payment
	
	 • Make the following information available to Cardholder about each Transaction in the Installment Transaction series, at minimum, through a website:
	   – Description of each individual purchase, including the name of the seller
	   – Amount and date of each individual purchase
	   – Amount of each Installment Transaction
	   – Number of installments paid and number of installments remaining
	   – MCC 5999 (Miscellaneous and Specialty Retail Stores) must be assigned

Advance Payment	Only the following Merchant categories may process an Advance

Table 5-21: Transaction-Specific Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials (Effective 25 January 2020) (continued)

Transaction Type	Requirement
	Payment representing the entire purchase amount before the goods or services are delivered: • T&E • Custom goods or services • Face-to-Face Environment, where not all items purchased in the Transaction are immediately available but will be shipped or provided at a later date • Recreational services or activities related to tourism and travel The terms and conditions must specify the date of shipping of the goods or services to the Cardholder.

Recurring Transaction	The Merchant must do all of the following:
	
	 • Provide a simple cancellation procedure, and, if the Cardholder's order was initially accepted online, at least an online cancellation procedure.
	
	 • Include the fixed dates or intervals on which the Transactions will be processed.
	
	 • At least 7 days before a Recurring Transaction, notify the Cardholder via email or other agreed method of communication if any of the following:
	
	   – **Effective 18 April 2020** A trial period, introductory offer, or promotional period is going to end. The Merchant must include in the communication the Transaction amount and Transaction Date of subsequent Recurring Transactions and a link or other simple mechanism to enable the Cardholder to easily cancel Transactions online or via SMS/text message.
	
	   – In the Europe Region: Any of the following:
	
	     ▪ More than 6 months have elapsed since the previous Recurring Transaction.
	
	     ▪ The Recurring Transaction agreement has been changed, including the amount of the Recurring Transaction, the date of the Recurring Transaction, or any other terms of the agreement.

Table 5-21: Transaction-Specific Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials (Effective 25 January 2020) (continued)

Transaction Type	Requirement
	▪ **Effective through 17 April 2020** A trial period, introductory offer, or promotional period is going to end. The Merchant must include in the communication the Transaction amount and Transaction Date of subsequent Recurring Transactions and a link or other simple mechanism to enable the Cardholder to easily cancel Transactions online or via SMS/text message.
Installment Transaction	Except as specified in the *Visa International Certificate of Incorporation and By-Laws,* Visa assumes no liability for an Installment Transaction processed more than 30 calendar days from the Authorization date.
¹ In the Europe Region: Or within the European Economic Area (EEA), to suppliers in the EEA	

Additionally, a Merchant or its agent that processes Transactions using a Stored Credential must comply with *Table 5-22, Processing Requirements for Transactions Using Stored Credentials (Effective 25 January 2020).*

Table 5-22: Processing Requirements for Transactions Using Stored Credentials (Effective 25 January 2020)

Requirement	Description
Before storing the credential	After a Cardholder agreement has been completed in writing, and before the first Transaction occurs, a Merchant must either: • Submit an Authorization Request for the Transaction amount • If payment is not required, submit an Account Verification For a Recurring Transaction, Installment Transaction, or Unscheduled Credential-on-File Transaction, use the appropriate indicator in the POS environment field. If the initial Authorization Request or Account Verification is not approved, the Merchant must not store the credential.
General Processing Requirements	• Before processing a Cardholder-initiated Transaction, the Merchant or its agent must also validate the Cardholder's identity (for example: with a login ID and password). • The Authorization amount must not exceed the individual Transaction amount or Partial Payment amount, as applicable.

Table 5-22: Processing Requirements for Transactions Using Stored Credentials (Effective 25 January 2020) (continued)

Requirement	Description

	• A Transaction with a Stored Credential must both:
	  – Use POS Entry Mode code 10
	  – For a Recurring Transaction, Installment Transaction, or Unscheduled Credential-on-File Transaction, use the appropriate indicator in the POS environment field.

Authorization Request Declines	If an Authorization Request for a Merchant-initiated Transaction with a Stored Credential is declined, the Merchant must notify the Cardholder in writing and allow the Cardholder at least 7 calendar days to pay by other means.

5.9.10.2 Mobile Phone Airtime Advance Payment – Europe Region (United Kingdom)

In the Europe Region (United Kingdom): To accept a Transaction for the purchase of prepaid mobile phone airtime in a Card-Absent Environment, a Merchant must do all of the following:

- Register no more than 2 Cards per mobile phone account, and no more than 2 mobile phone accounts per Card
- Obtain the Cardholder's name and home address
- Check the Card Verification Value 2 (CVV2) and Address Verification Service (AVS) data
- For a Recurring Transaction, all of the following:
  - Establish only one Recurring Transaction agreement per mobile phone account
  - Authenticate the initial Recurring Transaction by either:
    - Visa Secure – Electronic Commerce Indicator 5
    - CVV2/AVS checks
  - Conduct a new CVV2/AVS data check if the Cardholder's Stored Credential changes

CVV2/AVS checks are not required on subsequent Recurring Transactions when all of the following criteria are met:

- The account of the Card is one of the 2 registered to that mobile phone account.

- CVV2/AVS data was submitted as part of a previous Transaction for prepaid mobile phone airtime, made on the same account of the registered Card, and confirmed as matched by the Issuer at least 3 months before setting up the Recurring Transaction.

- The maximum amount of GBP 30 per calendar month is not exceeded.

If an Issuer charges back a Transaction, the Acquirer must inform the Merchant, and the Merchant must:

- Block the mobile phone account(s) for which the fraudulent Advance Payment was made

- Cancel the Card registration

- Not reregister a Card with the same Payment Credential

ID# 0030056   Edition: Apr 2020 | Last Updated: Apr 2020

5.9.11   Visa Easy Payment Service (VEPS) Transactions

5.9.11.1   Visa Easy Payment Service (VEPS) Transaction Qualifying Criteria

A Visa Easy Payment Service (VEPS) Transaction must comply with all of the following:

- Be conducted in a Card-Present Environment with a POS Entry Mode 05, 07, 90 or 91

- Be authorized

- Not be any of the following Transaction types:
    - An ATM Cash Disbursement Transaction
    - A Cash-Back Transaction
    - A Manual Cash Disbursement
    - A Quasi-Cash Transaction
    - A Transaction where Dynamic Currency Conversion (DCC) is performed
    - An Automated Fuel Dispenser (AFD) Transaction

- Not exceed the Transaction amount limit (including taxes, if applicable, and surcharge, if permitted) specified in *Section 5.9.11.2, Maximum Transaction Amounts for Visa Easy Payment Service (VEPS) Transactions and Transactions at Certain Contactless-Only Acceptance Devices*

- Be conducted using an eligible MCC, as specified in *Table 5-23, Eligible MCCs for VEPS Transactions*

Table 5-23: Eligible MCCs for VEPS Transactions

Region	Transaction	Environment or Transaction Type	Eligible MCCs
AP Region, Canada Region, CEMEA Region, Europe Region (Israel), LAC Region, US Region	All	Card-Present Environment	All MCCs
Europe Region (excluding Israel)	Contactless	Card-Present Environment	All MCCs
	Contact Chip and Magnetic Stripe	Unattended Transactions	• 4111 (Local and Suburban Commuter Passenger Transportation, including Ferries) • 4112 (Passenger Railways) • 4131 (Bus Lines) • 4784 (Tolls and Bridge Fees) • 7523 (Parking Lots, Parking Meters and Garages)

5.9.11.2   Maximum Transaction Amounts for Visa Easy Payment Service (VEPS) Transactions and Transactions at Certain Contactless-Only Acceptance Devices

The following maximum Transaction amounts apply to VEPS Transactions and Transactions at certain Contactless-only Acceptance Devices:

Table 5-24: VEPS Maximum Transaction Amounts – Europe Region

Country/Territory	Contact Chip or Magnetic-Stripe	Contactless or Contactless-Only
All countries: Face-to-Face Transactions with any MCC	0 (except Israel, see below)	EUR 20[1] (unless listed below)
All countries: Unattended	0 (except Israel, see below)	EUR 20[1]

Table 5-24: VEPS Maximum Transaction Amounts – Europe Region (continued)

Country/Territory	Contact Chip or Magnetic-Stripe	Contactless or Contactless-Only
Transactions with any MCC except MCC 4111, 4112, 4131, 4784, or 7523		(unless listed below)
All countries: Unattended Transactions with MCC 4111, 4112, 4131, 4784, or 7523	Contact Chip EUR 50[1] (unless listed below) Magnetic Stripe EUR 40[1] (unless listed below)	EUR 50[1] (unless listed below)
Austria	EUR 25	EUR 25
Belgium	**Effective 15 April 2020** EUR 50 (Domestic Transactions) **Effective 16 October 2020** EUR 25 (International Transactions)	**Effective 15 April 2020** EUR 50 (Domestic Transactions) **Effective 16 October 2020** EUR 25 (International Transactions)
Bulgaria	**Effective through 26 March 2020** BGN 50 (Domestic Transactions) **Effective 27 March 2020** BGN 100 (Domestic Transactions) BGN 50 (International Transactions)	**Effective through 26 March 2020** BGN 50 (Domestic Transactions) **Effective 27 March 2020** BGN 100 (Domestic Transactions) BGN 50 (International Transactions)
Croatia	**Effective through 20 April 2020** HRK 100 (Domestic Transactions) **Effective 21 April 2020** HRK 250 (Domestic Transactions) HRK 100 (International Transactions)	**Effective through 20 April 2020** HRK 100 (Domestic Transactions) **Effective 21 April 2020** HRK 250 (Domestic Transactions) HRK 100 (International Transactions)
Cyprus	**Effective 27 March 2020** EUR 50 (Domestic Transactions)	**Effective 27 March 2020** EUR 50 (Domestic Transactions)
Czech Republic	CZK 500	CZK 500
Denmark	DKK 350	DKK 350
Estonia	EUR 25	EUR 25
Finland	EUR 50	EUR 50

Table 5-24: VEPS Maximum Transaction Amounts – Europe Region (continued)

Country/Territory	Contact Chip or Magnetic-Stripe	Contactless or Contactless-Only
Germany	EUR 50	EUR 50
Greece	**Effective through 22 March 2020** EUR 25 (Domestic Transactions) **Effective 23 March 2020** EUR 50 (Domestic Transactions) EUR 25 (International Transactions)	**Effective through 22 March 2020** EUR 25 (Domestic Transactions) **Effective 23 March 2020** EUR 50 (Domestic Transactions) EUR 25 (International Transactions)
Hungary	**Effective through 26 March 2020** HUF 5,000 (Domestic Transactions) **Effective 27 March 2020** HUF 15,000 (Domestic Transactions) HUF 5,000 (International Transactions)	**Effective through 26 March 2020** HUF 5,000 (Domestic Transactions) **Effective 27 March 2020** HUF 15,000 (Domestic Transactions) HUF 5,000 (International Transactions)
Iceland	**Effective through 5 April 2020** ISK 5,000 (Domestic Transactions) **Effective 6 April 2020** ISK 7,500 (Domestic Transactions) ISK 5,000 (International Transactions)	**Effective through 5 April 2020** ISK 5,000 (Domestic Transactions) **Effective 6 April 2020** ISK 7,500 (Domestic Transactions) ISK 5,000 (International Transactions)
Israel	EUR 20[1]	EUR 20[1]
Italy	EUR 25	EUR 25
Latvia	EUR 25	EUR 25
Lithuania	EUR 25	EUR 25
Luxembourg	EUR 50	EUR 50
Malta	**Effective 23 March 2020** EUR 50 (Domestic Transactions)	**Effective 23 March 2020** EUR 50 (Domestic Transactions)
Netherlands	EUR 25	EUR 25
Norway	NOK 400	NOK 400

Table 5-24: VEPS Maximum Transaction Amounts – Europe Region (continued)

Country/Territory	Contact Chip or Magnetic-Stripe	Contactless or Contactless-Only
Poland	**Effective through 18 March 2020** PLN 50 **Effective 19 March 2020** PLN 100	**Effective through 18 March 2020** PLN 50 **Effective 19 March 2020** PLN 100
Portugal	**Effective 23 March 2020** EUR 50 (Domestic Transactions)	**Effective 23 March 2020** EUR 50 (Domestic Transactions)
Republic of Ireland	**Effective through 22 March 2020** EUR 15 (Domestic Transactions) **Effective 23 March 2020** EUR 50 (Domestic Transactions) EUR 15 (International Transactions)	**Effective through 22 March 2020** EUR 30 (Domestic Transactions) **Effective 23 March 2020** EUR 50 (Domestic Transactions) EUR 30 (International Transactions)
Romania	RON 100	RON 100
Slovenia	EUR 25	EUR 25
Sweden	**Effective through 16 April 2020** SEK 200 **Effective 17 April 2020** SEK 400	**Effective through 16 April 2020** SEK 200 **Effective 17 April 2020** SEK 400
Switzerland	CHF 40	CHF 40
Turkey	**Effective through 22 March 2020** TRY 120 (Domestic Transactions) **Effective 23 March 2020** TRY 250 (Domestic Transactions) **Effective through 16 April 2020** TRY 90 (International Transactions) **Effective 17 April 2020** TRY 120 (International Transactions)	**Effective through 22 March 2020** TRY 120 (Domestic Transactions) **Effective 23 March 2020** TRY 250 (Domestic Transactions) **Effective through 16 April 2020** TRY 90 (International Transactions) **Effective 17 April 2020** TRY 120 (International Transactions)
United Kingdom	**Effective through 31 March 2020** GBP 20 (Domestic Transactions) **Effective 1 April 2020**	**Effective through 31 March 2020** GBP 30 (Domestic Transactions) **Effective 1 April 2020**

Table 5-24: VEPS Maximum Transaction Amounts – Europe Region (continued)

Country/Territory	Contact Chip or Magnetic-Stripe	Contactless or Contactless-Only
	GBP 45 (Domestic Transactions)	GBP 45 (Domestic Transactions)
	GBP 20 (International Transactions)	GBP 30 (International Transactions)
[1] Or the equivalent amount in the Transaction Currency		

ID# 0027503   Edition: Apr 2020 | Last Updated: Apr 2020

5.9.12   Debt Repayment

5.9.12.1   Repayment of Debt

An Acquirer must ensure that a Debt repayment Transaction complies with all of the following:

Table 5-25: Debt Repayment Transaction Requirements

Requirement	Description
Prohibitions	• Use of a Credit Card or charge Card • Debt that exceeds the statute of limitations and is no longer collectible in a lawsuit, unless the Merchant obtains written Cardholder agreement to the charge and the amount

Restrictions	• For Debt that has been charged-off and transferred from the original owner to a third party, the Merchant must be either:
	  – A regulated financial institution
	  – Located in the Europe Region and a member of a professional body or association that creates industry standards
	
	• For payday lending,[1] the Merchant must be both:
	  – Located in the Europe Region
	  – A member of a recognized professional body or association

Processing Requirements	• Include the Debt repayment indicator in the Authorization Request and Clearing Record • Assign MCC 6012 (Financial Institutions – Merchandise, Services, and Debt Repayment) or MCC 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [not Money Transfer], Travelers Cheques, and

Visa Product and Service Rules

5 Acceptance

Visa Core Rules and Visa Product and Service Rules

Table 5-25: Debt Repayment Transaction Requirements (continued)

Requirement	Description
	Debt Repayment)
	• Complete the Transaction as a purchase
	• In the Europe Region: In a Card-Absent Environment:
	– The first Transaction must be Cardholder-initiated.
	– The first and all subsequent Cardholder-initiated Transactions must either:
	▪ Use 3-D Secure
	▪ Include all of the following data in the Authorization Request:
	▪ Date of birth of recipient account holder
	▪ Recipient account number (either partially masked or up to 10 characters)
	▪ Last name of recipient account holder
	▪ In the United Kingdom: Partial postcode of recipient account holder (numbers from the postcode only)
Resubmissions	A Debt repayment Transaction that receives a Decline Response may not be resubmitted for Authorization if any of the following:
	• The Transaction has already been submitted 3 times with each retry resulting in a Decline Response.
	• After more than 14 calendar days from the date of the original Decline Response
	• If the Decline Response code is one of the following:
	– 04 (Pickup card)
	– 14 (Invalid account number (no such number))
	– 41 (Pickup card (lost card))
	– 43 (Pickup card (stolen card))
	– 52 (No checking account)
	– 57 (Transaction not permitted to cardholder)
	– 75 (Allowable number of PIN-entry tries exceeded)
	– 78 (Blocked, first used)
	– 82 (Negative Online CAM, dCVV, iCVV, or CVV results)
	The Merchant must not deposit the Transaction if an Approval Response is received after

Table 5-25: Debt Repayment Transaction Requirements (continued)

Requirement	Description
	a Decline Response that meets one of these conditions.

In the Europe Region (United Kingdom): A Merchant or Acquirer may accept a Card, including a Credit Card, for the repayment of Debt that is considered overdue[2] only if it complies with all of the following:

- Has as its principal business the collection of overdue Debts

- Is a Member of its recognized professional body or association

- Uses MCC 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [not Money Transfer], Travelers Cheques, and Debt Repayment)

- Includes the Debt repayment indicator in the Authorization Request and Clearing Record

- For an Electronic Commerce Transaction, uses 3-D Secure to Authenticate the Cardholder when initiating, at a minimum, the first Transaction

[1] A loan or advance either as defined by local law or where the consumer is required to repay the loan or advance within 60 days, either as a single repayment or as a repayment in a fixed amount and the total amount paid by the consumer to extinguish the Debt or obligation substantially exceeds the original amount borrowed or advanced.

[2] For example: payments to a collection agency or in an attempt to recover funds for a dishonored check

ID# 0003026   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.9.13   Health Care

5.9.13.1   Preauthorized Health Care Transactions – US Region

In the US Region: For a Preauthorized Health Care Transaction, a Health Care Merchant must obtain from the Cardholder an Order Form that contains all of the following:

- A description of the requested services

- Permission for the Health Care Merchant to charge the Cardholder's account for the balance due following the Merchant's receipt of any applicable insurance payment

- Time period (not to exceed one year) for which permission is granted

A Health Care Merchant must not request Authorization for the amount due until it has received notification of adjudication from the Cardholder's insurance company.

ID# 0008706   **Edition: Apr 2020 | Last Updated: Oct 2014**

5.9.13.2   Acquirer Participation in Healthcare Auto-Substantiation – US Region

In the US Region: To process a Healthcare Auto-Substantiation Transaction, an Acquirer or its agent must comply with all of the following:

- Be licensed and certified by SIGIS

- Provide the Visa Flexible Spending Account (FSA) or Visa Health Reimbursement Arrangement (HRA) BIN list only to eligible Merchants

- Ensure that HRA and FSA Auto-Substantiation Transactions originate only from a SIGIS-certified Merchant

- Provide an IIAS Merchant Verification Value to the Merchant and include it in the Authorization Request

- Comply with all SIGIS requirements, including storage and fulfillment of Transaction Receipt data

- Fulfill Retrieval Requests for Transaction Receipt data associated with Visa Healthcare Auto-Substantiation Transactions. The Fulfillment must not be processed using Visa Resolve Online.

ID# 0003106   Edition: Apr 2020 | Last Updated: Oct 2016

5.9.13.3   Merchant Participation in Healthcare Auto-Substantiation – US Region

In the US Region: A Merchant that participates in Healthcare Auto-Substantiation must comply with all of the following:

- Be licensed and certified by SIGIS

ID# 0025549   Edition: Apr 2020 | Last Updated: Oct 2016

5.9.14   Visa Fleet Card

5.9.14.1   Visa Fleet Card Acquirer and Merchant Requirements – Canada and CEMEA Regions

In the Canada Region, CEMEA Region: An Acquirer that agrees to support the Visa Fleet Card Product must ensure the Visa Fleet Card Application Identifier (AID), and the appropriate terminal application is implemented in the terminal of its Merchant that wants to support Visa Fleet Card Transactions.

A Visa Fleet Card Acquirer must ensure that its Merchant that agrees to support Visa Fleet Card Transactions both:

- Modify POS Systems to support the Visa Fleet Card Application Identifier (AID)
- Modify POS systems to prompt and/or validate the Enhanced Data, and to pass on the Enhanced Data

ID# 0029231	Edition: Apr 2020 | Last Updated: Oct 2015

5.9.14.2   Visa Fleet Card Merchant Requirements – US Region

In the US Region: A Merchant that accepts a Visa Fleet Card must both:

- Prompt the Cardholder to provide the data required by the service prompt indicator
- Pass complete and accurate prompt-input data with the Visa Fleet Card Enhanced Data

ID# 0027525	Edition: Apr 2020 | Last Updated: Oct 2014

5.9.16   Up-Selling and Negative Option Merchants

5.9.16.1   Up-Selling Transaction Requirements

Effective through 17 April 2020 In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: An up-selling Merchant[1] must comply with all of the following:

- Clearly disclose to the Cardholder all of the following:
  - The name of the up-selling Merchant offering the goods and services in a manner that clearly differentiates the up-selling Merchant from the initial Merchant
  - A description of the goods and services
  - The length of any trial period, including clear disclosure that the Cardholder will be charged unless the Cardholder takes steps to cancel the subsequent Transaction
  - The Transaction amount and Transaction Date
  - The cancellation policy
- Obtain the Cardholder's express informed consent for any subsequent Transactions by requiring the Cardholder to do all of the following:
  - Enter the Cardholder's Payment Credential for the subsequent Transactions
  - Enter the Cardholder's name, address, and contact information
  - Perform an additional confirmatory action to indicate consent to the Transaction (for example: clicking a confirmation button)
- Comply with all other Transaction processing requirements

Effective 18 April 2020 For a Transaction involving up-selling[1], both of the following must occur:

- Before completing a Transaction, the initial Merchant must do all of the following:

  – Clearly disclose to the Cardholder all of the information specified in *Table 5-26, Required Disclosure/Transaction Receipt/Notification Content and Format for Up-Selling Transactions*. If the first Transaction is an Electronic Commerce Transaction, this information must be clearly visible on the checkout screen.

  – At the time of the first Transaction, obtain express Cardholder consent for any subsequent Transactions. If the first Transaction is an Electronic Commerce Transaction, consent must be obtained via a "click-to-accept" button on the checkout screen.

  – Immediately after the first Transaction has been completed, send a Transaction Receipt to the Cardholder as specified in *Table 5-26, Required Disclosure/Transaction Receipt/Notification Content and Format for Up-Selling Transactions*.

- At least 7 days before initiating a subsequent Transaction, the up-selling Merchant must provide to the Cardholder written notification as specified in *Table 5-26, Required Disclosure/Transaction Receipt/Notification Content and Format for Up-Selling Transactions*, if either:

  – The terms of the agreement between the Merchant and the Cardholder have changed. The notification must also include the new terms and conditions.

  – A trial period, introductory offer, or promotional period is going to end.

Table 5-26: Required Disclosure/Transaction Receipt/Notification Content and Format for Up-Selling Transactions

Required Content and Format for Up-Selling Transactions
Required Content
- The name of the up-selling Merchant offering the goods and services in a manner that clearly differentiates the up-selling Merchant from the initial Merchant   - A description of the goods and services   - The length of any trial period, introductory offer, or promotional period   - Clear disclosure that the Cardholder will be charged unless the Cardholder takes steps to cancel any subsequent Transactions   - The Transaction amount   - The Transaction Date   - Last 4 digits of the Payment Credential   - The cancellation policy

---

Table 5-26: Required Disclosure/Transaction Receipt/Notification Content and Format for Up-Selling Trans-actions (continued)

Required Content and Format for Up-Selling Transactions
• Instructions for an easy way to cancel the agreement and/or any subsequent Transactions
Required Format
If the first Transaction is an Electronic Commerce Transaction, the Merchant must send the Transaction Receipt or relevant notification electronically.

[1]   The sale of goods and services different from, and not affiliated with or a subsidiary of, the initial Merchant with whom the Cardholder initiates the Transaction.

ID# 0026364   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.9.16.2   Negative Option Transaction Requirements

Effective through 17 April 2020 In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Negative Option Merchant must comply with all of the following:

- Obtain the Cardholder's express informed consent by disclosing all purchase terms and conditions before initiating the initial Transaction, including, but not limited to, the following:
  – The name of the Merchant offering the goods and services
  – A description of the goods and services
  – The Transaction amount and Transaction Date (including for each recurring charge)
  – The length of any trial period, including clear disclosure that the Cardholder will be charged unless the Cardholder takes steps to cancel the subsequent Transaction
  – The cancellation policy
- Provide a simple mechanism for the Cardholder to cancel charges
- Comply with all other Transaction requirements

Effective 18 April 2020 A negative option Merchant[1] must do all of the following:

- Before completing an agreement or Transaction, clearly disclose to the Cardholder all of the information specified in *Table 5-27, Required Disclosure/Transaction Receipt/Notification Content and Format for Negative Option Transactions.* If the initial Transaction is an Electronic Commerce Transaction, this information must be clearly visible on the checkout screen.

- At the time of the agreement or first Transaction, obtain express Cardholder consent for any subsequent Transactions. If the first Transaction is an Electronic Commerce Transaction, consent must be obtained via a "click-to-accept" button on the checkout screen.

- Immediately after the first Transaction (if applicable) and Cardholder consent to subsequent Transactions, send to the Cardholder a Transaction Receipt (if applicable) or written confirmation, as specified in *Table 5-27, Required Disclosure/Transaction Receipt/Notification Content and Format for Negative Option Transactions*.

- At least 7 days before initiating a subsequent Transaction, provide written notification to the Cardholder as specified in *Table 5-27, Required Disclosure/Transaction Receipt/Notification Content and Format for Negative Option Transactions,* if either:

  – The terms of the agreement between the Merchant and the Cardholder have changed. The notification must also include the new terms and conditions.

  – A trial period, introductory offer, or promotional period is going to end.

Table 5-27: Required Disclosure/Transaction Receipt/Notification Content and Format for Negative Option Transactions

Required Content and Format for Negative Option Transactions
Required Content
- The name of the Merchant offering the goods and services   - A description of the goods and services   - The length of any trial period, introductory offer, or promotional period   - Clear disclosure that the Cardholder will be charged unless the Cardholder takes steps to cancel any subsequent Transactions   - The Transaction amount and Transaction Date for the initial Transaction (even if no amount is due) and for any subsequent Recurring Transactions   - Last 4 digits of the Payment Credential   - The cancellation policy   - Instructions for an easy way to cancel the agreement and/or any subsequent Transactions   - If the Merchant sends a Transaction Receipt or notification via email, a link to a page on the Merchant's website where the agreement, order, or any subsequent Transactions can be easily cancelled.
Required Format
If Cardholder consent to future Transactions occurred through a website or an application, the Merchant must send all Transaction Receipts and notifications electronically.

---

[1] A Merchant that requires a Cardholder to expressly reject the Merchant's offer of additional goods and/or services during the Transaction process or expressly decline to participate in future Transactions.

ID# 0026365   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.9.17   Gambling

5.9.17.1   Online Gambling Merchant and Acquirer Requirements

An Online Gambling Merchant must both:

- Have a valid license or other appropriate authority to operate its website and/or application
- Identify an Online Gambling Transaction with all of the following:
    - MCC 7995 (Betting), even when gambling services are not the Merchant's primary business
    - In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Identify the Transaction with the Quasi-Cash/Online Gambling Transaction indicator
    - In the Europe Region: Identify the Transaction as an Online Gambling Transaction in the Authorization Request and Clearing Record

If a Member, Merchant, Payment Facilitator, or Sponsored Merchant is unable to distinguish an Online Gambling Transaction from other Transactions, it must both:

- Identify all Transactions as Online Gambling Transactions
- Inform the Cardholder that Transactions may be identified on the billing statement as gambling Transactions

---

ID# 0002474   **Edition: Apr 2020 | Last Updated: Apr 2019**

5.9.17.2   Use of Funds Transfer for Online Gambling

If a funds transfer to an individual is to be used for an Online Gambling Transaction, an Acquirer must identify the funds transfer Transaction as an Online Gambling Transaction.

The Acquirer must have processes to identify and eliminate abuse by an individual, funds transfer Merchant, or Online Gambling Merchant that attempts to circumvent proper Transaction identification.

If Visa determines that an individual is facilitating Online Gambling Transactions through funds transfers, Visa may impose these requirements on the funds transfer Merchant for any future funds transfers to that individual.

ID# 0002955   **Edition: Apr 2020 | Last Updated: Oct 2014**

5.9.17.3   Disbursement of Gambling Winnings to a Cardholder

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A gambling Merchant must not deposit a Credit Transaction to disburse gambling winnings to a Cardholder except for an Original Credit Transaction.

In the Europe Region: A gambling Merchant must disburse gambling winnings to a Cardholder using an Original Credit Transaction and not in the form of cash, a check, or any other payment method.

If a gambling Merchant uses an Original Credit Transaction to disburse gambling winnings to a Cardholder, it must ensure that both the:

- Original Credit Transaction is processed to the same Payment Credential that was used to place the winning wager
- Transaction representing the winning wager was lawfully made, properly identified, and processed according to the Visa Rules

In the US Region: Gambling winnings disbursed to a Prepaid Card are not required to be issued to the same Payment Credential that initiated the wager, but must comply with all of the following:

- Be submitted by a gambling Merchant authorized by the Issuer to disburse winnings via a program that has been approved by Visa
- Be transmitted to the Issuer using a funding mechanism approved by Visa
- Represent a Transaction for the winning wager that was lawfully made, properly identified, and processed according to Visa Rules

ID# 0002958 | **Edition: Apr 2020 | Last Updated: Apr 2020**

5.9.17.4   Acquirer Requirements for Gambling Transactions in Norway – Europe Region

In the Europe Region: An Acquirer that acquires gambling Transactions in Norway must ensure that gambling Transactions are conducted only at Merchants licensed by the Norwegian Gaming Authority.

ID# 0030012 | **Edition: Apr 2020 | Last Updated: Apr 2019**

5.9.18   Mass Transit

5.9.18.1   Mass Transit Transaction Authorization Requirements

A Merchant performing a Mass Transit Transaction must submit an Online Authorization Request either:

- At the end of each Travel Period

- In the Europe Region: If any of the following conditions apply:

  - The Card was used for the first time at the Merchant or more than 14 calendar days have elapsed since Online Authorization was last requested for the Payment Credential by the Merchant.

  - The Chip on the Card requested Online Authorization at any point during the Travel Period.

  - The cumulative value of a Mass Transit Transaction since the last Online Authorization Request by the Merchant for the Payment Credential is equal to or greater than the Mass Transit Transaction cumulative offline limit.[1]

[1] This limit is set to the same value as the Contactless Floor Limit in that country.

ID# 0030049	Edition: Apr 2020 | Last Updated: Apr 2020

5.9.18.2   Mass Transit Transaction Requirements

An Acquirer must ensure that its Merchants that perform Mass Transit Transactions do all of the following:

- Register with Visa

- Deploy Contactless-only Acceptance Devices

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Are able to receive a Payment Account Reference (PAR)

- In the Europe Region: Are able to receive a Payment Account Reference (PAR)

- Submit an Account Verification when a Card is first used at the Merchant

- Block a Card from being used for travel within one hour of receiving either:

  - A Decline Response

  - An Issuer response to an Account Verification indicating that the Transaction should not be completed with that Card

- Reset the Mass Transit Transaction parameters held for a Card on the Merchant's host system and/or remove any travel block on the Card only after receiving an Approval Response to an Authorization Request that contained Full-Chip Data

- Upon completion of a Transaction, provide the Cardholder with access to all of the following information for a minimum of 120 days following the Transaction Processing Date:

  – Merchant name

  – Total Transaction amount in the Transaction Currency

  – Details of each individual journey completed during the Travel Period, including the start and end time of each journey

  – Final Transaction Date

  – Any discounts applied

To obtain an Approval Response following a Decline Response, the Merchant must request Online Authorization using either of the following amounts:

- If no fare is outstanding, the Transaction amount that was cleared following the Decline Response. Upon receipt of an Approval Response, the travel block must be removed within one hour and the Authorization Request must be reversed.

- The amount of any outstanding fare. Upon receipt of an Approval Response, the travel block must be removed within one hour.

ID# 0030050	Edition: Apr 2020 | Last Updated: Apr 2020

5.9.19   Visa Rent Payment Program – US Region

5.9.19.1   Visa Rent Payment Program – US Region

Effective 18 April 2020 In the US Region: To participate in the Visa Rent Payment Program, an Acquirer must do all of the following:

- Register with Visa and provide the specific amount or percentage of the fee assessed by each Merchant or Sponsored Merchant, by product

- Ensure that only a Merchant or Sponsored Merchant classified with MCC 6513 (Real Estate Agents and Managers) participates in the program

- Obtain a Merchant Verification Value (MVV) for each participating Merchant or Payment Facilitator and include it in the Authorization Request and Clearing Record

- Process all Visa rent payment program Transactions through VisaNet

A participating Merchant or Sponsored Merchant (including through their Payment Facilitator) may assess a fee to the Cardholder only in the Card-Absent Environment for either a single Transaction or Recurring Transaction(s).

- If assessed for a Visa Debit Card Transaction, the fee must comply with all of the following:
  - Not exceed USD 10
  - Included in the final Transaction amount and in the surcharge field of the Clearing Record
  - Be clearly disclosed to the Cardholder before the completion of the Transaction. The Cardholder must be given the opportunity to cancel after the fee is disclosed.
  - Not be assessed in addition to a Service Fee, a Convenience Fee, or any other fee
  - Not required to be equally applied to an alternative method of payment
  - Not be greater than a fee applied to any other general purpose payment debit card
- If assessed for a Visa Credit Card Transaction, the fee must comply with all of the following as though the fee is deemed a Surcharge:
  - *Section 5.6.1.4, Similar Treatment of Visa Transactions – US Region and US Territories*
  - *Section 5.6.1.7, US Credit Card Surcharge Disclosure Requirements – US Region and US Territories*

ID# 0030673	Edition: Apr 2020 | Last Updated: New

5.10   Transaction Receipt Requirements

5.10.1   Transaction Receipt Delivery to Cardholders

5.10.1.1   Transaction Receipt Delivery to Cardholders

A Merchant or Acquirer must provide[1] a completed Transaction Receipt to a Cardholder, as follows:

Table 5-28: Transaction Receipt Delivery to Cardholders

Transaction Type	Transaction Receipt Required	When Transaction Receipt Must Be Provided
For all Transactions, unless otherwise specified	Yes, if requested by Cardholder	At the time of the Transaction

Table 5-28: Transaction Receipt Delivery to Cardholders (continued)

Transaction Type	Transaction Receipt Required	When Transaction Receipt Must Be Provided
The Merchant initiates the Transaction, including any of the following: • Deferred Payment Transactions • Recurring Transactions • Installment Transactions • Unscheduled Credential-on-File Transactions	Yes	At the time of the Transaction
The Cardholder initiates the Transaction, and any of the following: • The Transaction Receipt contains a restricted return, refund, or exchange policy • The Merchant requires the Transaction Receipt if the Cardholder returns merchandise • The Transaction is a Dynamic Currency Conversion Transaction • The Transaction is a Plus ATM Shared Deposit Transaction	Yes	At the time of the Transaction
The Transaction is any of the following: • Expedited exit Transactions at an amusement park • Express-return Transactions at a rental Merchant • Priority check-out Transactions at a Cruise Line or Lodging Merchant	Yes	Within 3 business days of a Cardholder's departure, check-out, disembarkation, or rental return
An Unattended Cardholder-Activated Terminal Transaction, excluding an Automated Fuel Dispenser (AFD) Transaction, that is either: • For an amount less than or equal to USD 25 (or local currency equivalent) • A Telephone Service Transaction with MCC 4814 (Telecommunication Service)	No	N/A

Visa Product and Service Rules

5 Acceptance

Visa Core Rules and Visa Product and Service Rules

If required to provide a Transaction Receipt to the Cardholder, the Merchant must provide a Transaction Receipt as follows:

- For an Electronic Commerce Transaction, a Mail/Phone Order Transaction, or a Transaction that occurs at a Contactless-only Acceptance Device, the Merchant may choose to offer only paper or only electronic Transaction Receipts. This does not apply to a Contactless-only Acceptance Device used for donations.

- For all other Transactions, the Merchant must offer a paper Transaction Receipt unless the Cardholder agrees to an electronic Transaction Receipt

[1] For a Mobile Push Payment Transaction, instead of the Merchant or Acquirer, an Issuer must provide an electronic Transaction Receipt to the Cardholder, as specified in, *Section 8.5.1.2, Electronic Transaction Receipt Requirements for Mobile Push Payment Transactions*

ID# 0027835   Edition: Apr 2020 | Last Updated: Oct 2019

5.10.1.2   Electronic Format Cardholder Receipt Delivery Requirements

If a Merchant provides an electronic Transaction Receipt to a Cardholder, the Merchant must do all of the following:

- If a link to a website and/or application is provided, all of the following:
  - Provide clear instructions to the Cardholder for accessing the Transaction Receipt
  - Ensure that the link is a direct link to the Transaction Receipt
  - Make the receipt available to the Cardholder for at least 120 calendar days after the Processing Date

- Provide instructions to enable the Cardholder to obtain the receipt if the Cardholder does not receive it

- Not store or use personal information provided by the Cardholder to enable the Merchant to provide the receipt for any other purpose without the express consent of the Cardholder

- Include both of the following in the title of the email or the title or first line of the wirelessly delivered message:
  - The Merchant name as it will appear in the Clearing Record and on the Cardholder billing statement
  - Language indicating that the email or wirelessly-delivered message contains the Cardholder's copy of a Transaction Receipt or a link to the Cardholder's copy of a Transaction Receipt

- Provide the receipt in a static format that cannot be easily manipulated after it has been created

ID# 0027837   Edition: Apr 2020 | Last Updated: Apr 2018

5.10.2   Transaction Receipt Retention Period

5.10.2.1   Transaction Receipt Retention Period

For Transactions in which a Merchant or Acquirer must obtain Cardholder signature, the Merchant or Acquirer must retain a Transaction Receipt for a minimum of 120 calendar days after the Processing Date.

ID# 0028051	Edition: Apr 2020 | Last Updated: Oct 2019

5.10.3   Transaction Receipt Data and Format Requirements

5.10.3.1   Prohibited Transaction Receipt Content for All Transactions

A Transaction Receipt must not contain:

- If the Transaction Receipt bears the Visa Program Marks, promotional, advertising, or similar language that conveys preference of a non-Visa payment card
- More information than is embossed or printed on the Card. This does not apply to any of the following:
  - A Token
  - A Card on which only a partial Account Number is printed
  - A Card on which no Account Number is printed

ID# 0026206	Edition: Apr 2020 | Last Updated: Apr 2020

5.10.3.2   Required Transaction Receipt Content for All Transactions

A Transaction Receipt must include all of the following elements:

Table 5-29: Required Transaction Receipt Content for All Transactions

Required Element	Additional Requirements
Payment Credential[1]	The Payment Credential, except for the final 4 digits, must be disguised or suppressed on the Cardholder's copy of a Transaction Receipt.
Authorization Code	Applies only to Transactions that were authorized by the Issuer[1]
Card network name	Must contain "Visa"[2]
Cardholder	This applies to a Transaction only if all of the following apply:

Table 5-29: Required Transaction Receipt Content for All Transactions (continued)

Required Element	Additional Requirements
signature on Merchant/Acquirer Copy	• The Transaction occurs in a Face-to-Face Environment. • The Transaction takes place at a Magnetic-Stripe-only Acceptance Device. • The Transaction is not a Visa Easy Payment Service (VEPS) Transaction. • A PIN is not used to verify the Cardholder.
Description of goods or services[1]	Description of the purchase
Merchant, Marketplace, or Digital Wallet Operator (DWO) location[1]	• For a Transaction involving a Merchant Outlet or Marketplace, the city and state/province of the Merchant Outlet or Marketplace • For an ATM Transaction, the location or street address of the ATM
Acquirer, Consumer Bill Payment Service (CBPS), DWO, Marketplace, or Merchant name	• The name used by the Merchant to identify itself to its customers, except for the following: – For an ATM Transaction, the name of the ATM Acquirer – For a Transaction involving a Payment Facilitator or High-Risk Internet Payment Facilitator the name of the Payment Facilitator and the name of the Sponsored Merchant (or an abbreviation) – For a back-to-back Transaction involving a retailer signed by a Staged Digital Wallet Operator (SDWO), the name of the SDWO and the name of the retailer – For a Transaction involving a Marketplace, the name of the Marketplace and the name of the retailer – **Effective 18 April 2020** For a Transaction involving an up-selling Merchant, the name of the up-selling Merchant offering the goods and services in a manner that clearly differentiates the up-selling Merchant from the initial Merchant – **Effective 17 October 2020** For a Transaction involving a CBPS, the name of the CBPS and the name of the biller
Return and refund policies	As specified in *Section 5.4.2.4, Disclosure to Cardholders of Return, Refund, and Cancellation Policies*
Transaction amount and Transaction currency symbol[3]	Total currency amount of all goods and services sold to the Cardholder at the same time, including applicable taxes and fees and any adjustments or credits

Table 5-29: Required Transaction Receipt Content for All Transactions (continued)

Required Element	Additional Requirements
	The currency symbol denoting the Transaction Currency, if the Transaction Currency is not the local currency of the Transaction Country
Transaction Date	No additional requirements
Transaction type[1]	One of the following: • ATM Cash Disbursement • Cash-Back with no purchase • Credit • Manual Cash Disbursement • Prepaid Load • Purchase
Other details embossed on Card[1]	Applies only to the Merchant copy of a manually imprinted Transaction Receipt

[1] This does not apply to a Visa Easy Payment Service (VEPS) Transaction.

[2] In the US Region or US Territory: This does not apply to a Transaction initiated using the Visa US Common Debit Application Identifier of a US Covered Visa Debit Card, when the processing network is not known at the time that the Transaction Receipt is generated. The Transaction Receipt must contain the application label selected (either "Visa Debit" or "US Debit," as applicable) or another enhanced descriptor.

[3] If the currency symbol or identification is not on the Transaction Receipt, the Transaction Currency is the local currency of the Transaction Country.

ID# 0027843   **Edition: Apr 2020 | Last Updated: Apr 2020**

5.10.3.3   Required Transaction Receipt Content for Specific Transaction Types

In addition to the requirements in *Section 5.10.3.2, Required Transaction Receipt Content for All Transactions*, and *Section 5.4.2.4, Disclosure to Cardholders of Return, Refund, and Cancellation Policies,* a Transaction Receipt must contain all of the following, as applicable:

Table 5-30: Required Transaction Receipt Content for Specific Transactions

Transaction Type	Required Content
Effective 25 January 2020	• For a full Advance Payment:

Table 5-30: Required Transaction Receipt Content for Specific Transactions (continued)

Transaction Type	Required Content
Advance Payment	– Full cancellation and refund policy, including the date and time that any refund privileges expire without Advance Payment forfeiture – Advance Payment Transaction amount – Scheduled start date or delivery date of the goods or services – The word(s) "Advance Payment" or "Prepayment" – For cancellations, cancellation confirmation • For a partial Advance Payment: – Full cancellation and refund policy, including the date and time that any refund privileges expire without Advance Payment forfeiture – Advance Payment Transaction amount – The word(s) "Advance Payment," "Deposit," or "Partial Payment" if there is a balance outstanding – For balance payments, the word "Balance" if the full remaining cost of the goods or services has been paid • For cancellations, cancellation confirmation
Aggregated Transaction	• Amount of each individual purchase • Date of each individual purchase • Description of each individual purchase
Airline Transaction	For ticket purchases, itinerary data
ATM Cash Disbursement/Shared Deposit Transaction	• Balance[1] • Type of account accessed • If an Access Fee is charged: – The words "ATM Fee," "Terminal Fee," or "Access Fee"[2] – In the US Region, Canada Region: Identification of the Acquirer as the recipient of the fee • In the Europe Region: In addition, all of the following: – ATM or Load Device Acquirer name and/or name of affiliated domestic or regional network

Table 5-30: Required Transaction Receipt Content for Specific Transactions (continued)

Transaction Type	Required Content
	– ATM or Load Device street location or location code – ATM or Load Device city
Transaction at a rental Merchant	• Daily rental rate • Any applicable taxes • Dates of pick-up and return • Description of additional costs
Cash-Back Transaction	Cash-back amount shown separately to purchase amount
Chip Transaction (Europe Region)	• Application Preferred Name[3] or Application Label[3] (if present on the Card)
Cruise Line Transaction	• Cabin rate • Dates of embarkation and disembarkation
Debt Repayment Transaction	Type of repayment (for example: "loan," "mortgage," "credit card," "goods," "services")

Dynamic Currency Conversion Transaction	• Transaction amount, with currency symbols, in:
	  – Merchant's or ATM's local currency
	  – Transaction Currency
	• Words "Transaction Currency" or "Transaction Amount" next to the Transaction amount
	• Currency Conversion Rate
	• Currency conversion commission, fees, or markup on the exchange rate over a wholesale rate or government-mandated rate
	• Statement, easily visible to the Cardholder, that the Cardholder has been offered a choice of currencies for payment (including the local currency of the Merchant or the currency dispensed at the ATM) and expressly agrees to the Transaction
	• Statement that Dynamic Currency Conversion is conducted by the Merchant or ATM Acquirer

Electronic Commerce	• Customer service contact

Table 5-30: Required Transaction Receipt Content for Specific Transactions (continued)

Transaction Type	Required Content
Transaction	- Merchant country - Merchant online address - Conditions of sale, including return and cancellation policy
Visa Fleet Card Transaction	- In the Canada Region,[4] CEMEA Region,[4] US Region: – Fuel product code – Fuel quantity – Fuel type – Fuel unit price – Odometer reading – The time of the Transaction[5]
Lodging Merchant Transaction (in which lodging is a component)	- Dates of check-in and check-out - Daily room charge - Any applicable taxes - Description and dates of individual purchases
Manual Cash Disbursements and Quasi-Cash Transactions	**Effective through 16 October 2021** 4 digits printed below the Account Number (if present) - Type of secondary identification (for example: passport, driver's license) without including the number or any other identifying information - For a Manual Cash Disbursement, the words "Cash Disbursement"
No-Show Transaction	- Daily room charge or rental rate - Taxes - Agreed start date of the accommodation or rental - The words "No Show"
Effective 25 January 2020 Partial Payment	- Name of the seller, if the Merchant is not the seller of the goods or services being purchased - A number representing where the Transaction falls in the installment sequence (for example: "2 of 4")

Table 5-30: Required Transaction Receipt Content for Specific Transactions (continued)

Transaction Type	Required Content
Preauthorized Healthcare Transaction (US Region)	For a Healthcare Auto-Substantiation Transaction, the words "Preauthorized Healthcare"
Effective through 24 January 2020 Prepayment Transaction	For a full prepayment: • Full cancellation and refund policy, including the date and time that any refund privileges expire without prepayment forfeiture • Prepayment amount • Scheduled start date or delivery date of the merchandise or services • The word "Prepayment" For a partial prepayment: • Full cancellation and refund policy, including the date and time that any refund privileges expire without prepayment forfeiture • Prepayment amount • The word(s) "Deposit" or "Partial Payment" if there is a balance outstanding • For balance payments, the word "Balance" if the full remaining cost of the goods or services has been paid • For cancellations, cancellation confirmation
Effective 18 April 2020 Transaction (or establishment of an agreement if no amount is due at the time the Stored Credential is captured) involving a trial period, introductory offer, or promotional period	• The length of any trial period, introductory offer, or promotional period, including clear disclosure that the Cardholder will be charged unless the Cardholder takes steps to cancel any subsequent Transactions • The Transaction amount and Transaction Date for the initial Transaction (even if no amount is due) and for subsequent Recurring Transactions • A link or other simple mechanism to enable the Cardholder to easily cancel the Transaction and any subsequent Transactions online or via SMS/text message
Transaction on which a fee is assessed (where permitted)	Shown separately and clearly: • Convenience Fee • Service Fee

Table 5-30: Required Transaction Receipt Content for Specific Transactions (continued)

Transaction Type	Required Content
	• Surcharge. The amount must be shown separately on the front of the receipt in the same type and size of font as other wording on the Transaction Receipt. • Wire Transfer Money Order Fee • Any other fees Fees and Surcharges must not be identified as a Visa-imposed charge.
Visa Mobile Prepaid Transaction (confirmation message)	Available balance in the Visa Mobile Prepaid account

[1] In the Europe Region: Required only for a Transaction with a Prepaid Card

[2] In the Europe Region: This does not apply.

[3] Not required for a Visa Easy Payment Service Transaction

[4] For a Merchant that supports a Visa Fleet Transaction through the Visa Fleet Card Application Identifier

[5] In the Canada Region, CEMEA Region: **Effective 17 October 2020**

ID# 0028052   Edition: Apr 2020 | Last Updated: Apr 2020

5.11   Returns, Credits, and Refunds

5.11.1   Merchant Processing

5.11.1.1   Merchant Processing of Credits to Cardholders

A Merchant that processes a credit to a Cardholder for a valid Transaction that was previously processed, must do all of the following:

• Send an Authorization Request[1] for the amount of the Credit Transaction, as specified in *Table 5-31, Thresholds for Merchant Credit Transaction Authorization Requests*

• Deliver a completed Credit Transaction Receipt to the Cardholder

Table 5-31: Thresholds for Merchant Credit Transaction Authorization Requests

Region	Merchants with Estimated Annualized Visa Purchase Return Sales Volume Equal to or Greater than:	All Merchants
AP	**Effective through 17 April 2020** USD 1 million	**Effective 18 April 2020**
Canada	**Effective through 18 October 2019** USD 5 million	**Effective 19 October 2019**
CEMEA	**Effective through 17 April 2020** USD 1 million	**Effective 18 April 2020**
Europe	N/A	**Effective 18 April 2020**
LAC	N/A	**Effective 19 October 2019**
US	**Effective through 18 October 2019** USD 10 million	**Effective 19 October 2019**

[1] Optional for Airlines and Mass Transit Merchants

ID# 0008605	Edition: Apr 2020 | Last Updated: Apr 2020

5.11.1.2   Credit Refunds for Timeshares

A timeshare Merchant must provide a full credit refund when the Cardholder cancelled the Transaction within 14 calendar days of the contract date or the date the contract or related documents were received.

ID# 0003082	Edition: Apr 2020 | Last Updated: Oct 2015

5.11.1.3   Prohibition of Resubmission of Returned Transaction

A Merchant must not submit a Transaction to the Acquirer that was previously disputed and subsequently returned to the Merchant. However, the Merchant may pursue payment from the customer outside the Visa system.

ID# 0003022	Edition: Apr 2020 | Last Updated: Apr 2018

5.11.1.4   Sales Tax Rebates

A Merchant that provides a sales tax rebate[1] to a Cardholder must process the rebate as an Original Credit Transaction.

A Merchant that offers Dynamic Currency Conversion (DCC) for a sales tax rebate must comply with all DCC requirements.

[1] A rebate of only the tax paid on the purchase, including value-added tax (VAT), goods and services tax (GST), or other general consumption tax that is rebated to the Cardholder.

ID# 0030025   Edition: Apr 2020 | Last Updated: Apr 2018

5.12   Acquirer Requirements for Non-Visa General Purpose Payment Network – LAC Region (Brazil)

In the LAC Region (Brazil): An Acquirer must not discriminate against any non-Visa general purpose payment network.

An Acquirer that contracts with a non-Visa general purpose payment network must do all of the following:

- Ensure that the non-Visa general purpose payment network complies with all of the following:
  - Is authorized by the Brazil Central Bank
  - Has a contract with Visa
  - Only processes funds transfer transactions

- Assign MCC 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [not Money Transfer], Travelers Cheques, and Debt Repayment) to the funds transfer transactions processed by the non-Visa general purpose payment network

- Ensure that the Merchant name field includes the message "transferência" and the name of the non-Visa general purpose payment network (or an abbreviation)

ID# 0029510   Edition: Apr 2020 | Last Updated: Apr 2018

5.13   Payment Solution Providers

5.13.1   Acquirer Requirements for Consumer Bill Payment Service Providers

Effective 17 October 2020 An Acquirer that contracts with a Consumer Bill Payment Service (CBPS) provider[1] must do all of the following:

- Register the CBPS with Visa and obtain written approval for each CBPS before processing any Transactions as a CBPS. Visa may, at its sole discretion, determine whether a third-party biller is eligible to participate in the CBPS program.

- Certify that the CBPS qualifies as a CBPS and complies with the Visa Rules

- Meet a minimum equity requirement of USD 100 million[2]

- Conduct an adequate due diligence review of the CBPS and the non-Visa-accepting billers to ensure compliance with the Acquirer's obligation to submit only legal Transactions to VisaNet and to ensure that the CBPS engages only in legal transactions with such billers.

- Communicate to Visa the Merchant name and the Card acceptor identification assigned to the CBPS, and consistently use them in all Transaction messages

- Populate an identifier associated with the CBPS on every participating Transaction

- Ensure that if the CBPS applies a Service Fee the underlying biller is located in a permitted country and uses a permitted MCC, as specified in *Section 5.6.3.1, Service Fee Assessment Requirements – Canada, CEMEA (Egypt, Russia), LAC (Trinidad and Tobago), and US Regions*

- Upon Visa request, provide to Visa activity reporting on each CBPS, including all of the following:

  – CBPS name

  – Biller name

  – Biller location

  – Monthly Transaction count and amount for each biller

  – Any other data requested by Visa

- Ensure that the CBPS:

  – In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Makes payments only to billers that are businesses located in the same country as the CBPS

  – In the Europe Region: Makes payments to billers that are businesses located in the same country as the CBPS or to billers that are businesses located in any country in the European Economic Area (EEA), if the CBPS and Acquirer have the necessary approvals to do business in the country where the biller is located

  – Uses the appropriate MCC to identify a biller, as listed in *Table 5-32, Consumer Bill Payment Service Provider – Allowed MCCs*. If unable to use the biller MCC or meet the requirements, the biller is ineligible for the program and must use MCC 4829.

  – Performs customer verification (KYC) and meets all applicable anti-money laundering requirements for all non-Visa-accepting billers before initiating Transactions for such billers

  – Only aggregates payments to a single biller

- If using a Card to pay billers for the associated bill payment, only uses a Visa Commercial Card if the Cardholder paid using a Visa Commercial Card

- Clearly discloses to the Cardholder, before the Transaction takes place, that it is the Merchant and that the Transaction involves only the transfer of money from the Cardholder to the third party

- Upon completion of a Transaction, provide the Cardholder with access to all of the following information for at least 120 days following the Transaction Processing Date:
  - Biller name
  - Total Transaction amount in the Transaction Currency
  - Transaction Date
  - Biller payment date and method
- Ensure that all Transactions processed by a CBPS include both:
  - CBPS name and biller name in the Merchant name field
  - CBPS identifier

Table 5-32: Consumer Bill Payment Service Provider – Allowed MCCs

Country	Allowed MCCs
AP Region	
Australia, New Zealand, Singapore	Any of the following: • 4900 (Utilities – Electric, Gas, Water, and Sanitary) • 6012 (Financial Institutions – Merchandise, Services, and Debt Repayment) • 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [Not Money Transfer], Account Funding [not Stored Value Load], Travelers Cheques, and Debt Repayment) • 6513 (Real Estate Agents and Managers – Rentals) • 6300 (Insurance Sales, Underwriting, and Premiums) • 8211 (Elementary and Secondary Schools) • 8220 (Colleges, Universities, Professional Schools, and Junior Colleges) • 8241 (Correspondence Schools) • 8244 (Business and Secretarial Schools) • 8249 (Trade and Vocational Schools)

Table 5-32: Consumer Bill Payment Service Provider – Allowed MCCs (continued)

Country	Allowed MCCs
	• 8299 (Schools and Educational Services [Not Elsewhere Classified]) • 9311 (Tax Payments)
Canada Region	
Canada	Any of the following: • 4900 (Utilities – Electric, Gas, Water, and Sanitary) • 6513 (Real Estate Agents and Managers – Rentals) • 8211(Elementary and Secondary Schools) • 8220 (Colleges, Universities, Professional Schools, and Junior Colleges) • 8241 (Correspondence Schools) • 8244 (Business and Secretarial Schools) • 8249 (Trade and Vocational Schools) • 8299 (Schools and Educational Services [Not Elsewhere Classified]) • 9311 (Tax Payments)
Europe Region	
European Economic Area (EEA) Countries Only	Any of the following: • 4814 (Telecommunication Services) • 4900 (Utilities – Electric, Gas, Water, and Sanitary) • 6012 (Financial Institutions – Merchandise, Services, and Debt Repayment) • 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [Not Money Transfer], Account Funding [not Stored Value Load], Travelers Cheques, and Debt Repayment) • 6513 (Real Estate Agents and Managers – Rentals) • 8011 (Doctors and Physicians [Not Elsewhere Classified]) • 8050 (Nursing and Personal Care Facilities) • 8062 (Hospitals) • 8099 (Medical Services and Health Practitioners [Not Elsewhere Classified]) • 8211 (Elementary and Secondary Schools)

Table 5-32: Consumer Bill Payment Service Provider – Allowed MCCs (continued)

Country	Allowed MCCs
	• 8220 (Colleges, Universities, Professional Schools, and Junior Colleges) • 8241 (Correspondence Schools) • 8244 (Business and Secretarial Schools) • 8249 (Trade and Vocational Schools) • 8299 (Schools and Educational Services [Not Elsewhere Classified]) • 9311 (Tax Payments)
LAC Region	
Brazil	Any of the following: • 4814 (Telecommunication Services) • 4899 (Cable, Satellite, and Other Pay Television/Radio/Streaming Services) • 4900 (Utilities – Electric, Gas, Water, and Sanitary) • 6300 (Insurance Sales, Underwriting, and Premiums) • 6513 (Real Estate Agents and Managers – Rentals) • 8211 (Elementary and Secondary Schools) • 8220 (Colleges, Universities, Professional Schools, and Junior Colleges) • 8241 (Correspondence Schools) • 8244 (Business and Secretarial Schools) • 8249 (Trade and Vocational Schools) • 8299 (Schools and Educational Services [Not Elsewhere Classified]) • 9311 (Tax Payments)
US Region	
US	Any of the following: • 4900 (Utilities – Electric, Gas, Water, and Sanitary) • 6012 (Financial Institutions – Merchandise, Services, and Debt Repayment) • 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [Not Money Transfer], Account Funding [not Stored Value Load], Travelers Cheques, and Debt Repayment)

Table 5-32: Consumer Bill Payment Service Provider – Allowed MCCs (continued)

Country	Allowed MCCs
	• 6513 (Real Estate Agents and Managers – Rentals)
	• 8011 (Doctors and Physicians [Not Elsewhere Classified])
	• 8050 (Nursing and Personal Care Facilities)
	• 8062 (Hospitals)
	• 8099 (Medical Services and Health Practitioners [Not Elsewhere Classified])
	• 8211 (Elementary and Secondary Schools)
	• 8220 (Colleges, Universities, Professional Schools, and Junior Colleges)
	• 8241 (Correspondence Schools)
	• 8244 (Business and Secretarial Schools)
	• 8249 (Trade and Vocational Schools)
	• 8299 (Schools and Educational Services [Not Elsewhere Classified])
	• 9311 (Tax Payments)

[1] A Merchant that provides a payment solution that allows Cardholders to pay qualifying billers. A biller may or may not be a Merchant.

[2] Visa may waive this requirement in exchange for assurance and evidence of the imposition of risk controls and requirements satisfactory to Visa. Such controls and requirements may include, but are not limited to, the pledging of additional collateral.

ID# 0030635   Edition: Apr 2020 | Last Updated: Apr 2020

5.13.2   Acquirer Responsibilities Related to Business Payment Solution Providers

5.13.2.1   Acquirer Requirements for Business Payment Solution Providers

An Acquirer that contracts with a Business Payment Solution Provider (BPSP)[1] must do all of the following:

- Register the BPSP with Visa
- Certify that the BPSP qualifies as a BPSP and complies with the Visa Rules
- **Effective 18 April 2020** Meet a minimum equity requirement of USD 100 million[2]

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Process only Domestic Transactions for the BPSP

- In the Europe Region: Process only Domestic Transactions and intra-European Economic Area Transactions for the BPSP

- Process BPSP Transactions with MCC 7399 (Business Services [Not Elsewhere Classified])

- Conduct an adequate due diligence review of the BPSP and the non-Visa-accepting suppliers to ensure compliance with the Acquirer's obligation to submit only legal Transactions to VisaNet and to ensure the BPSP engages only in legal transactions with such suppliers.

- Communicate to Visa the Merchant name and the Card acceptor identification assigned to the BPSP, and consistently use them in all Transaction messages

- Upon Visa request, provide to Visa activity reporting on each BPSP and each non-Visa-accepting supplier, including:

  – Supplier name

  – Supplier location

  – BPSP name

  – Monthly Transaction count and amount

  – Any other data requested by Visa

- Ensure that the BPSP:

  – Makes payments only to suppliers[3] that are businesses located in the same country[4] as the BPSP in accordance with the buyer's payment instruction

  – Initiates a Transaction only after the buyer has confirmed that the non-Visa-accepting supplier has shipped goods or delivered services and the buyer has approved the payment

  – Performs customer verification (KYC) and meets all applicable anti-money laundering requirements for all non-Visa-accepting suppliers before initiating Transactions for such suppliers' invoices

  – Uses a secure payment process that ensures funds are paid into individual supplier accounts

  – Ensures that each invoice from a non-Visa-accepting supplier to a buyer is processed as a separate Transaction

  – Contractually obligates the buyer, by way of written agreement between the buyer and the BPSP, to accept all risks associated with non-performance of the non-Visa-accepting supplier

Visa reserves the right to revoke a BPSP's registration for any reason

[1] An entity that provides a business-to-business payment solution that allows buyers to pay non-Visa accepting suppliers

with a Visa Commercial Card

2 Visa may waive this requirement in exchange for assurance and evidence of the imposition of risk controls and requirements satisfactory to Visa. Such controls and requirements may include, but are not limited to, the pledging of additional collateral.

3 Payments to a supplier that has been a Merchant within the previous 12 months are prohibited.

4 In the Europe Region: Or within the European Economic Area (EEA), to suppliers in the EEA

ID# 0030064   **Edition: Apr 2020 | Last Updated: Oct 2019**

6   ATM

6.1   Plus Program

6.1.1   Plus Program Issuer Participation Requirements

6.1.1.1   Plus Program Issuer Participation

To issue a Card with Plus functionality, an Issuer must do all of the following:

- Obtain a license to use the Plus Program Marks and comply with rules for using the Plus Symbol
- Provide Authorization service 24 hours a day, 7 days a week

ID# 0004060	Edition: Apr 2020 | Last Updated: Oct 2017

6.1.2   Plus Symbol

6.1.2.1   Plus Program Marks on Cards

A Member must use the Plus Symbol only as a Mark indicating acceptance for ATM services.

An Issuer of a Proprietary Card bearing the Plus Symbol must place the Plus Symbol on all Proprietary Cards within 5 years from the beginning date of participation in the Plus Program.

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: The presence of the Plus Symbol is optional on a Visa Card or non-Visa-branded Campus Card if no other ATM acceptance Mark is present on the Card.

ID# 0003577	Edition: Apr 2020 | Last Updated: Oct 2016

6.1.2.2   Restrictions on the Use of other Marks on Plus Cards – AP, Canada, CEMEA, LAC and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Card bearing the Plus Symbol must not bear the Marks of any entity ineligible for membership in Visa, or of any of the following entities, or their subsidiaries or affiliates, deemed competitive by Visa:[1]

- American Express Company
- Discover Financial Services[2]

- JCB

- MasterCard Worldwide

A Card bearing the Plus Symbol is exempt from this requirement if it was issued under an agreement executed with Visa or Plus System, Inc. before 1 October 1992.

A Card bearing the Plus Symbol must not bear a Trade Name or Mark confusingly similar to any other Visa-Owned Mark.

[1] In the US Region or a US Territory: A US Covered Visa Debit Card bearing the Plus Symbol may bear the Marks of entities deemed competitive by Visa, as specified in the _Visa Product Brand Standards_.

[2] In the US Region: This does not apply to Visa Cards bearing the Pulse Mark and Cards bearing the Plus Symbol.

ID# 0006159	**Edition: Apr 2020 | Last Updated: Oct 2016**

6.1.2.3   Plus Symbol Displayed at an ATM

The Plus Symbol must be displayed at an ATM that accepts Plus-enabled Cards for ATM services.

ID# 0003583	**Edition: Apr 2020 | Last Updated: Oct 2017**

6.2   Visa Global ATM Network

6.2.1   Visa Global ATM Network Issuer Participation Requirements

6.2.1.1   Visa Global ATM Network Issuer Participation

To participate in the Visa Global ATM Network, an Issuer must successfully complete certification with Visa. Rules regarding Visa Issuer participation in the Visa Global ATM Network apply to all Visa Cards.

In the US Region: A Visa Consumer Card Issuer must participate in the Visa ATM Network.

ID# 0004070	**Edition: Apr 2020 | Last Updated: Oct 2017**

6.2.2   Visa Global ATM Network Issuer General Requirements

6.2.2.2   Custom Payment Services/ATM Program Issuer Participation

An Issuer that participates in the Custom Payment Services/ATM must do all of the following:

- Complete Issuer certification

- Receive and return the ATM Transaction Identifier in each Transaction

- Receive the terminal ID code, ATM owner, and ATM location data in each Transaction record

- Include the ATM Transaction Identifier in all Disputes

ID# 0004078	Edition: Apr 2020 | Last Updated: Apr 2018

6.2.3   Visa Global ATM Network Acquirer Participation Requirements

6.2.3.1   Visa Global ATM Network Acquirer Participation

Any ATM owned, leased, sponsored, or controlled by a Member is eligible for participation in the Visa Global ATM Network.

A Member that sponsors a non-Member agent to deploy or operate an ATM participating in the Visa Global ATM Network must ensure that the non-Member agent complies with *Section 1.10.8.5, Third Party Agent Contract,* and *Section 10.2.1.1, VisaNet Processor Contracts.*

An Acquirer that participates in the Visa ATM Network must both:

- Ensure that all of its ATMs that participate in other regional or national ATM networks also participate in the Visa Global ATM Network

- Display Visa ATM and Plus acceptance Marks on all ATMs within 30 days from the date the Acquirer begins accepting Visa Cards and Plus-enabled Cards

ID# 0004783	Edition: Apr 2020 | Last Updated: Apr 2019

6.2.3.2   ATM Cash Disbursement and Transaction Currency Requirements

An ATM Cash Disbursement is either:

- A Visa Transaction if it is completed with a Visa Card or a Visa Electron Card

- A Plus Transaction if it is completed with a non-Visa-branded card or a Plus-enabled Proprietary Card, and/or a Card enabled on the Plus network

An ATM must both:

- Disburse cash in the local currency or display the type of currency or travelers cheques dispensed

- Support a Cash Disbursement of at least USD 200 (or local currency equivalent) per day, per Account Number, and in a single Transaction upon Cardholder request

---

ID# 0029537 | Edition: Apr 2020 | Last Updated: Apr 2019

6.2.3.3   ATM Card Acceptance

An ATM Acquirer must accept all valid Cards for all Transaction functions in which the Acquirer has elected to participate through the Visa Global ATM Network.

In the Canada Region: This does not apply to a Member that participated in the Visa Global ATM Network as of 13 June 2013.

In the Canada Region: All ATM Acquirers that began participation in the Visa Global ATM Network after 14 June 2013 must accept all valid Cards.

At the discretion of Visa, an ATM Acquirer that accepts Plus-enabled Cards may selectively deny access to its ATMs.

An ATM Acquirer certified to accept Visa Cards may selectively deny access to its ATMs if the Card presented is both issued to residents of the country where the ATM is located and billed in the local currency.

An ATM with restricted access must display language with the Visa Brand Mark that both identifies the ATM Acquirer and describes Visa Card acceptance or the nature of any restrictions.

ID# 0004785 | Edition: Apr 2020 | Last Updated: Apr 2019

6.2.4   ATM Operator and Agent Requirements

6.2.4.1   Display of Member Name on Non-Member ATM – LAC Region

In the LAC Region: An ATM Acquirer must ensure that the name of the Member that operates or sponsors the ATM is prominently displayed on every non-Member ATM.

ID# 0004746 | Edition: Apr 2020 | Last Updated: Oct 2014

6.2.4.2   ATM Operator Agreement Requirements

An ATM Acquirer must have a written ATM Operator agreement with each of its ATM Operators[1] and must only process Visa ATM Network Transactions from an ATM Operator with which it has a valid agreement. The form, content, and appearance of an ATM Operator agreement are at the discretion of the ATM Acquirer, except as specified below. An ATM Operator agreement must include both:

- The ATM Acquirer's name, location, and contact information in letters consistent in size with the rest of the ATM Operator agreement, and in a manner that makes the ATM Acquirer's name readily visible to the ATM Operator

- Language stating that the ATM Operator may be terminated for failure to comply with the ATM Operator agreement

ATM Operator agreements must be made available to Visa upon request and must not contain contractual details regarding pricing arrangements.

[1] Tri-party agreements (ATM Acquirer, Agent, ATM Operator) are permitted.

ID# 0009021	Edition: Apr 2020 | Last Updated: Oct 2017

6.2.4.3   Acquirer Requirements for ATM Operators

Before entering into an ATM Operator agreement, an ATM Acquirer must determine that a prospective ATM Operator has no significant derogatory background information about any of its principals. The ATM Acquirer must:[1]

- Maintain documented policies and procedures to manage its Agent programs

- Validate its Agent's compliance with the ATM Acquirer solicitation and qualification standards on a quarterly basis

- Collect all of the following information from its ATM Operators and Agents:

    – "Doing Business As" (DBA) name

    – ATM Operator legal name

    – ATM Operator outlet location, including street address, city, state, and postal code

    – In the US Region: Federal Taxpayer Identification Number, Federal Employer Identification Number, or Social Security Number of all principals

    – Full first and last name and middle initial of principals (for example: of corporations, partnerships, sole proprietors)

    – Incorporation status (for example: corporation, partnership, sole proprietor, non-profit)

[1] An ATM Acquirer may allow its Agents to execute ATM Operator agreements on its behalf and conduct due diligence reviews.

ID# 0003510	Edition: Apr 2020 | Last Updated: Apr 2018

Visa Product and Service Rules

6.2.6   ATM Processing Requirements

6.2.6.1   ATM Acquirer Processing

Before acting as an ATM Acquirer, an Acquirer (including an Acquirer that processes through a VisaNet Processor with an existing VisaNet endpoint) must do all of the following:

- Comply with applicable licensing and processing requirements
- Be certified to participate in either the:
  - Single Message System[1]
  - Custom Payment Services/ATM

If the ATM Acquirer does not meet all tier II requirements, Visa may remove the ATM Acquirer from the tier II level.

[1] All ATM Acquirers in the US Region and all new ATM Acquirers (excluding an Acquirer that processes through a VisaNet Processor with an existing VisaNet endpoint) must process ATM Transactions using the Single Message System.

ID# 0008597   **Edition: Apr 2020 | Last Updated: Apr 2019**

6.2.6.3   ATM Misdispense

For a misdispense:

- A Custom Payment Services/ATM Acquirer must process an ATM confirmation message for the actual amount dispensed.
- A Single Message System ATM Acquirer must both:
  - **Effective through 17 April 2020** Process an Adjustment for the actual amount of the misdispense within 45 calendar days of the Processing Date of the original Transaction
  - **Effective 18 April 2020** Process an Adjustment for the actual amount of the misdispense within 10 calendar days of the Processing Date of the original Transaction. An Adjustment processed after 10 calendar days may be subject to a Dispute for late Presentment.
  - For an over-dispense caused by a misloaded terminal, attempt good-faith collection from the Issuer before processing an Adjustment to the Cardholder account

ID# 0002406   **Edition: Apr 2020 | Last Updated: Apr 2020**

6.2.6.4   ATM Transaction Reversal

The Reversal amount must be the original Transaction amount.

ID# 0002404	Edition: Apr 2020 | Last Updated: Oct 2015

6.2.6.5   ATM Transaction Adjustment Conditions

Effective 18 April 2020 An ATM Acquirer may not process more than 2 debit Adjustments if the Adjustments are related to multiple Reversals that were both:

- Processed on the same Account Number on the same Transaction Date.
- Processed using one of the following reason codes:
  - 2502 (Transaction has not completed [request or advice timed out or ATM malfunctioned])
  - 2503 (No confirmation from point of service)

ID# 0030670	Edition: Apr 2020 | Last Updated: New

6.2.6.6   ATM Account Number Acceptance

An ATM and a Member ATM processing system must accept all valid International Organization for Standardization numbers of 11-19 digits, starting with any digit from 0 through 9.

ID# 0004786	Edition: Apr 2020 | Last Updated: Oct 2014

6.2.6.7   ATM Transaction Processing

An ATM Acquirer must ensure all of the following:

- The entire, unaltered contents of track 2 of the Magnetic Stripe, or the Magnetic-Stripe Image from the Chip on the Card, are read and transmitted.

ID# 0004792	Edition: Apr 2020 | Last Updated: Oct 2017

6.2.6.8   ATM Transaction Authorization and Clearing Requirements

An Acquirer must ensure that both:

- An ATM Transaction cleared through VisaNet was also authorized through VisaNet.
- All of the following information matches in the Authorization and Clearing Record:
  - Account Number
  - Authorization Code
  - Acquiring Identifier

– Transaction amount

– Account Selection processing code

– MCC

ID# 0004795	Edition: Apr 2020	Last Updated: Oct 2019

6.2.6.9 ATM Account Range Table

An ATM Acquirer must do all of the following:

- Use the Visa Account Range table to determine the routing of an Authorization Request
- Install and use the table within 6 business days of its receipt from Visa
- Not disclose or distribute to any third party the ATM Account Range table

If an ATM Acquirer does not route all Transactions to Visa for Cards bearing the Plus Symbol, it must both:

- Install and use the Plus Account Range table within 3 business days of its receipt from Visa
- Use the Plus Account Range table to determine the routing of an Authorization Request for a Card bearing the Plus Symbol. This does not apply to licensees of the Plus System, Inc.

ID# 0008780	Edition: Apr 2020	Last Updated: Apr 2019

6.2.6.10 Decline of an ATM Authorization Based on Expiration Date

An ATM Acquirer must not return or decline an ATM Transaction based on the expiration date, and must ensure that an ATM Authorization Request originating from an Expired Card is sent Online to the Issuer for an Authorization Response.

ID# 0006005	Edition: Apr 2020	Last Updated: Oct 2014

6.2.6.12 ATM Transaction Timeout Time Limit

An ATM and its host system must not timeout a Transaction in less than 45 seconds.

ID# 0002405	Edition: Apr 2020	Last Updated: Oct 2014

6.2.6.13 Card Retention at an ATM

An ATM is not required to have the ability to retain Cards. If it does have this ability, it may retain a Card only upon the request of the Issuer.

If a Card is retained, an Acquirer must do all of the following:

- Log it under dual custody immediately after removal from the ATM

- Render the Card unusable, following secure Card destruction requirements, as specified in *Section 10.7.2.1, Recovered Card Handling and Notification Requirements*

- Notify the Issuer through Visa Resolve Online that the Card has been recovered, as specified in *Section 10.7.2.1, Recovered Card Handling and Notification Requirements*

ID# 0008063	Edition: Apr 2020	Last Updated: Apr 2017

6.2.6.14   Accidental Card Retention at an ATM

If a hardware or software failure causes mistaken or accidental Card retention, and to the extent possible, an ATM Acquirer must return the Card to the Cardholder after reviewing positive Cardholder identification and, where the Card contains a signature panel, comparing the Cardholder's signature to that on the Card signature panel.

If the Cardholder does not request the return of the Card within 7 days, the ATM Acquirer must follow Card retention rules as specified in *Section 6.2.6.13, Card Retention at an ATM,* and must not submit a Fee Collection Transaction for Recovered Card handling fee/reward (reason code 0150).

ID# 0007014	Edition: Apr 2020	Last Updated: Oct 2019

6.2.6.17   Visa Mobile Prepaid Acceptance for ATM Transactions

An ATM Acquirer that participates in Visa Mobile Prepaid:

- Must transmit all of the following to complete Transaction when the Card is absent:
  - Account Number
  - Expiration date
  - Valid PIN

- May choose to accept cardless Visa Mobile Prepaid ATM Transactions in addition to Transactions where the Card is present

- Is not required to read and transmit the contents of track 2 of the Magnetic Stripe or the Magnetic-Stripe Image from the Chip on the Card if the Transaction is initiated through key-entry by a Visa Mobile Prepaid account holder

ID# 0027683	Edition: Apr 2020	Last Updated: Oct 2019

6.3   ATM Optional Services

6.3.1   ATM Optional Services Issuer Participation

6.3.1.1   Issuer Participation in Optional ATM Services

To participate in account-to-account transfers, Balance Inquiry,[1] mini-statements, PIN change, and PIN unblock, an Issuer must do all of the following:

- Obtain certification from Visa

- Support the services as separate, non-financial transactions

- For Balance Inquiry, provide balances in the currency of the Cardholder's account, for conversion by Visa to the Transaction Currency

To participate in the Shared Deposit Service, an Issuer must comply with the requirements specified *Section 6.3.3.1, Issuer Participation in the Plus Shared Deposit Service.*

[1] An Issuer must support a Balance Inquiry Service if it supports Balance Inquiry for any network other than its proprietary network.

ID# 0004074	**Edition: Apr 2020 | Last Updated: Apr 2019**

6.3.1.2   Issuer Participation in the Access Fee-Free ATM Service

To participate in the Access Fee-free ATM service, an Issuer must submit to Visa a completed *Access Fee-Free Participation Agreement* and include a list of participating BINs/Account Ranges.

ID# 0030609	**Edition: Apr 2020 | Last Updated: Oct 2019**

6.3.2   ATM Optional Services Acquirer Participation

6.3.2.1   Acquirer Participation in Optional ATM Services

To participate in account-to-account transfers, Balance Inquiry,[1] mini-statements, PIN change, and PIN unblock, an ATM Acquirer must do all of the following:

- Obtain certification from Visa

- Support the services as separate, non-financial transactions

- For Balance Inquiry, display the balance in the currency of the ATM, either on the screen or on the receipt

An ATM Acquirer may supply the Cardholder with any balance information provided by the Issuer as part of an ATM Cash Disbursement.

To participate in the Shared Deposit Service, an Acquirer must comply with the requirements specified in *Section 6.3.3.2, Acquirer Participation in the Plus Shared Deposit Service.*

A participating ATM Acquirer receives a fee for each Shared Deposit, account-to-account transfer, Balance Inquiry, mini-statement, PIN change, or PIN unblock request.

[1]   An ATM Acquirer must support a Balance Inquiry Service if it supports Balance Inquiry for any network other than its proprietary network.

ID# 0004804	Edition: Apr 2020 | Last Updated: Oct 2019

6.3.2.2   Acquirer Participation in the Access Fee-Free ATM Service

To participate in the Access Fee-free ATM service, an Acquirer must comply with all of the following:

- Submit to Visa a completed *Access Fee-Free Participation Agreement* and include both:
  - Participating ATM locations
  - Related Acquiring Identifier(s)
- Honor all Cards that are not subject to an Access Fee
- Be able to identify participating BINs

ID# 0030608	Edition: Apr 2020 | Last Updated: Oct 2019

6.3.3   Plus ATM Shared Deposit Service

6.3.3.1   Issuer Participation in the Plus Shared Deposit Service

An Issuer that participates in the Shared Deposit Service must do all of the following:

- Honor all Adjustments submitted by the Acquirer, subject to Dispute rights, and make all reasonable attempts to collect the funds
- Upon enrollment and as information changes, provide contact names and telephone numbers to Visa for exception processing
- Decline a Transaction that exceeds the minimum or maximum deposit amount limits established by the Issuer

ID# 0030601	Edition: Apr 2020 | Last Updated: Apr 2019

6.3.3.2   Acquirer Participation in the Plus Shared Deposit Service

An Acquirer that participates in the Shared Deposit Service must both:

- Accept Shared Deposits at the same ATMs where it accepts any other network's deposits
- Certify itself, and ensure that all direct endpoints are certified, to participate in the Shared Deposit Service

The Acquirer may:

- Participate in the Shared Deposit Service without participating as an Issuer
- Include all or a portion of its owned ATMs for participation in the Shared Deposit Service

An ATM Acquirer that participates in another network's deposit-sharing arrangement must participate in the Plus ATM's Shared Deposit Service unless the Acquirer's participation in a deposit-sharing arrangement involves only a Proprietary Network.

ID# 0030597   Edition: Apr 2020 | Last Updated: Apr 2019

6.3.3.3   Shared Deposit Service – Acquirer Responsibilities

An ATM Acquirer that participates in the Shared Deposit Service, where permitted, must do all of the following:

- Collect deposits received through the service and verify their eligibility
- Act as the Cardholder's agent in transmitting the deposited funds to the Cardholder's institution
- Credit the Cardholder's institution via Plus network Settlement
- If assessing an Access Fee on the Shared Deposit Transaction, both:
  - Disclose the Access Fee on the Transaction Receipt and the ATM screen, as specified in *Section 5.10.3.3, Required Transaction Receipt Content for Specific Transaction Types*
  - Comply with the Access Fee requirements specified in *Section 6.4.1, ATM Access Fees*
- Maintain records for at least 2 years (or longer based on any applicable laws or regulations)
- Upon enrollment and as information changes, provide contact names and telephone numbers to Visa for exception processing
- Forward the deposit envelope (if applicable) and any ineligible deposits to the issuing institution in a reasonably secure manner
- Notify the Issuer of the receipt of a return item and, if applicable, return the original document to the Issuer no later than 45 calendar days from the date of Adjustment

---

ID# 0030596   Edition: Apr 2020 | Last Updated: Apr 2019

6.3.3.4   Credit Union-Only Shared Deposit Arrangements

A Plus Member that is a credit union that participates in another shared deposit arrangement may choose not to participate in Shared Deposits, if the Member participates in sharing arrangements that include only credit unions.

If such sharing arrangements include non-credit unions, a Member must participate in Shared Deposits.

ID# 0030595   Edition: Apr 2020 | Last Updated: Apr 2019

6.3.3.5   Shared Deposit Verification

An ATM Acquirer must verify and balance the Shared Deposits received at its ATMs within 2 business days of the Transaction Date. If the Transaction occurs on a non-business day, the count begins from the next official business day.

ID# 0030604   Edition: Apr 2020 | Last Updated: Apr 2019

6.3.3.6   Adjustments for Shared Deposit Transactions

An ATM Acquirer must submit separate Adjustments for each item that is deemed ineligible in a Shared Deposit. In limited instances, when warranted, the Acquirer may submit multiple Adjustments for a single Shared Deposit Transaction.

An Acquirer that processes a Shared Deposit Adjustment must comply with all of the following:

- Not submit an Adjustment for a Transaction that has been declined by the Issuer.
- For a debit Adjustment of a returned deposit or an ineligible deposit item, initiate the Adjustment within both:
  - 45 calendar days of the Transaction Date
  - One business day from either the receipt of the returned deposit or verification of the ineligible item, as applicable. An Adjustment submitted more than one business day after the receipt of a returned deposit or the verification of an ineligible deposit is considered a late Adjustment, and is subject to a processing fee.
- Not submit a Dispute Response for a late Adjustment of ineligible deposit items including, but not limited to, the following:

- – Empty envelope

- – Missing envelope

- – Non-negotiable items (or example: Transaction receipts, coupons, blank pieces of paper)

- – Foreign currency

- – Envelope contents that do not equal the amount shown on the deposit slip and/or envelope

- – Envelope contents that do not equal the amount shown in the ATM message

- Be liable for the late Adjustment processing fee, as specified in the applicable Fee Schedule

- Notify the Issuer within 24 hours of submitting an Adjustment that is over USD 500

- Not submit a Dispute Response if the Adjustment was previously disputed

- Return the original document(s) to the Issuer for a debit Adjustment relating to a returned item, ineligible deposit item, or foreign currency

- Post a credit Adjustment to the Cardholder's account as soon as possible upon determining that an item is ineligible

ID# 0030603	Edition: Apr 2020	Last Updated: Apr 2019

6.3.3.7   Shared Deposit Transaction Adjustment Reversal Timeframe

For a Shared Deposit Transaction, an ATM Acquirer must submit an Adjustment reversal within 10 calendar days of the Settlement Date of the original Adjustment.

ID# 0030671	Edition: Apr 2020	Last Updated: New

6.4   ATM Fees

6.4.1   ATM Access Fees

6.4.1.1   Domestic ATM Access Fees

An ATM Acquirer must not impose an Access Fee[1] on a domestic ATM Transaction unless either:

- The Transaction is a Shared Deposit Transaction

- Applicable laws or regulations expressly require that an ATM Acquirer be permitted to impose an Access Fee.[1]

Visa Core Rules and Visa Product and Service Rules

An ATM Acquirer in a country where an Access Fee for domestic ATM Cash Disbursements is permitted by Visa must comply with the requirements specified for International ATM Cash Disbursement Access Fees.

[1] In the AP Region (Australia, Thailand), Canada Region, LAC Region (Panama, Puerto Rico), US Region: This does not apply.

| ID# 0007996 | Edition: Apr 2020 | Last Updated: Apr 2019 |

6.4.1.2   Domestic ATM Access Fee – Canada Region

In the Canada Region: An ATM Acquirer may impose an Access Fee on a domestic ATM Cash Disbursement or a Shared Deposit Transaction.

An ATM Acquirer may impose an Access Fee if all of the following:

- It imposes an Access Fee on all other interchange transactions through other shared networks at the same ATM.
- The Access Fee is not greater than the Access Fee amount on all other interchange transactions through other shared networks at the same ATM.
- The Domestic Transaction is initiated by a Card issued by a Member other than the ATM Acquirer.
- The Access Fee is a fixed and flat fee.

| ID# 0004715 | Edition: Apr 2020 | Last Updated: Apr 2019 |

6.4.1.4   Domestic ATM Access Fees on Cash Disbursement – CEMEA Region (Russia)

In the CEMEA Region (Russia): An ATM Acquirer may impose an Access Fee on a domestic ATM Cash Disbursement if all of the following requirements are met:

- It imposes an Access Fee on all other domestic ATM Cash Disbursements through any other network at the same ATM.
- The Access Fee is not greater than the Access Fee amount on all other domestic transactions through any other network at the same ATM.
- The Access Fee is a fixed and flat fee.
- It includes the value of the dispensed cash and any Access Fee amount in the Authorization Request and Clearing Record.
- The dispensed cash and Access Fee amount are separately identified.
- It informs the Cardholder of the Access Fee amount and that the Access Fee is assessed in addition to the charges assessed by the Issuer.

- It requests Cardholder approval of the Access Fee and provides the ability to cancel the ATM Transaction.

ID# 0024130	Edition: Apr 2020	Last Updated: Apr 2019

6.4.1.5   Acquirer Requirements for ATM Access Fees

Visa reserves the right to request any of the following from an ATM Acquirer that imposes an Access Fee on international ATM Cash Disbursements or domestic Shared Deposit Transactions:

- Notice of intent to impose an Access Fee
- A report with the physical location of each ATM and the total number of ATMs at which an Access Fee is imposed
- Message display and language disclosure related to Access Fees
- Any other information required by applicable laws or regulations

An Acquirer that chooses to impose an ATM Access Fee must comply with all of the following:

Table 6-1: Acquirer and ATM Requirements for ATM Access Fees

Requirement Type	Requirements
Access Fees	- Impose the Access Fee only on the following Transactions: – International ATM Cash Disbursements, unless applicable laws or regulations expressly require that an ATM Acquirer be permitted to impose an Access Fee on domestic ATM Cash Disbursements – Shared Deposit Transactions - Impose the Access Fee on all other Shared Deposit Transactions or international ATM Cash Disbursements processed through any other network at the same ATM - Ensure that the Access Fee is not greater than the Access Fee amount on all other similar Transactions through any other network at the same ATM - Ensure that the Access Fee is a fixed and flat fee - Include the value of the dispensed cash or the Shared Deposit and any Access Fee amount in the Authorization Request and Clearing Record - Separately identify the dispensed cash or the Shared Deposit amount and the Access Fee amount
Disclosures	Inform the Cardholder that an Access Fee is assessed in addition to the charges assessed by the Issuer. The disclosure must comply with all of the following:

Visa Product and Service Rules

6 ATM

Visa Core Rules and Visa Product and Service Rules

Table 6-1: Acquirer and ATM Requirements for ATM Access Fees (continued)

Requirement Type	Requirements

	– Be in English and the local language equivalent
	
	– Be as high a contrast or resolution as any other graphics on the ATM
	
	– Use same font size as other headings and text on the terminal, and ensure it is legible
	
	– In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: Contain the notice: Fee Notice "(Member Name) will assess a fee to cardholders for international ATM Cash Disbursements. This fee is added to the amount of your transaction and is in addition to any fees that may be charged by your financial institution."
	
	– In the US Region: Both:
	
	  ▪ Contain the notice: Fee Notice – "(Acquirer/Member Name) charges a (USD amount) fee to US Cardholders for withdrawing cash. This fee is added to the amount of your withdrawal and is in addition to any fees that may be charged by your financial institution."
	
	  ▪ Be readily visible to the Cardholder in the Cardholder's line of sight
	
	– For a Shared Deposit Transaction, contain the notice: Fee Notice – "(Member Name) will assess a fee to cardholders for Shared Deposits. This fee is deducted from the amount of your deposit and is in addition to any fees that may be charged by your financial institution."
	
	• Identify the ATM Acquirer as the recipient of the Access Fee
	
	• Inform the Cardholder of the Access Fee amount before the Transaction takes place
	
	• Request Cardholder approval of the Access Fee
	
	• Provide the ability for the Cardholder to cancel the ATM Transaction

ID# 0030077   Edition: Apr 2020 | Last Updated: Oct 2019

Visa Product and Service Rules

6 ATM

Visa Core Rules and Visa Product and Service Rules

6.4.2   ATM Travelers Cheque Fee

6.4.2.1   ATM Travelers Cheque Fee Disclosure

If an ATM dispenses traveler's cheques and charges a fee, the Member must disclose the fee to the Cardholder.

ID# 0004800	Edition: Apr 2020	Last Updated: Oct 2014

7   Transaction Processing

7.1   VisaNet Systems Use

7.1.1   Use of VisaNet

7.1.1.1   Submission of Domestic Transactions to VisaNet – AP, Canada, CEMEA, LAC and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Unless prohibited by applicable laws or regulations, a Member must submit all Domestic Transactions, not otherwise submitted for Clearing or Settlement, to VisaNet as Collection-Only. This includes, but is not limited to, any Transaction that is processed as follows:

- Through one of the following:
  - A VisaNet Processor
  - A non-Visa network
  - A domestic switch or any other form of processor
- Under any domestic Private Agreement or bilateral agreement
- As an On-Us Transaction

The following Transaction types are not required to be submitted to VisaNet.[1] However, a Member may choose to submit:

- Domestic ATM Cash Disbursements
- Domestic Manual Cash Disbursements

[1] This does not apply to Domestic Transactions in the Canada Region or CEMEA Region (Nigeria).

ID# 0027827	Edition: Apr 2020 | Last Updated: Oct 2017

7.1.1.3   Required Use of VisaNet for Processing – AP Region

In the AP Region (Australia, Bangladesh,[1] Malaysia, Philippines, Singapore, Thailand, Vietnam): A Member must authorize, clear, and settle all Domestic Transactions through VisaNet.

In the AP Region (Australia): This does not apply to:

- On-Us Transactions

- Domestic Transactions in a Face-to-Face Environment, on a co-badged Visa Card, where the domestic debit network associated with the co-badged acceptance mark is selected

In the AP Region (Malaysia, Philippines, Singapore, Thailand, Vietnam): This does not apply to:

- ATM Transactions

- On-Us Manual Cash Disbursements

- Transactions on a co-badged Visa Card processed on the domestic debit network associated with the co-badged acceptance mark

In the AP Region (Malaysia, Philippines, Singapore, Thailand, Vietnam): This includes:

- On-Us Transactions

- Transactions processed through a VisaNet Processor or any other Agent

Effective 18 April 2020 In the AP Region (Bangladesh): This does not apply to:

- ATM Transactions

- On-Us Transactions

[1] **Effective 18 April 2020**

ID# 0026201	Edition: Apr 2020 | Last Updated: Apr 2020

7.1.1.4   Non-Visa Debit Transaction Disclosure Requirements – US Region

In the US Region: An Issuer that enables Non-Visa Debit Transactions to be processed without a PIN must clearly communicate to its Cardholders both:

- That it does not require all such transactions to be authenticated by a PIN

- The provisions of its Cardholder agreement relating only to Visa Transactions are not applicable to non-Visa transactions

At the time of issuance or implementation of such processing, this Cardholder communication must be included in the terms and conditions of the deposit and/or debit account.

ID# 0008884	Edition: Apr 2020 | Last Updated: Apr 2018

7.2   Access to Visa Systems

7.2.1   Visa Extended Access

7.2.1.1   Member Requirements for Visa Extended Access and Visa Extended Access Proxy

If a Member has Visa Extended Access, the Member must use it to transmit its Interchange.

A Member must not use Visa Extended Access or Visa Extended Access Proxy for any purpose other than to access VisaNet or a permitted Visa application, unless otherwise approved by Visa. A Member must not make or attempt to make any repair, adjustment, alteration, or modification to Visa Extended Access or Visa Extended Access Proxy.

ID# 0008744	Edition: Apr 2020 | Last Updated: Oct 2019

7.2.1.2   Member Support of Visa Extended Access and Visa Extended Access Proxy

A Member that participates in Visa Extended Access or Visa Extended Access Proxy must provide, at no cost to Visa, reasonable support requested by Visa for installing the V.I.P. System, BASE II, and/or other applicable Visa applications, including all of the following:

- Providing a location that meets Visa requirements for installing Visa Extended Access or Visa Extended Access Proxy on the Member's premises[1]

- Providing a sufficient number of qualified personnel that the Member will train to meet Visa specifications

- Maintaining V.I.P. System, BASE II, and/or other applicable Visa applications' records, documents, and logs required by Visa and providing them at Visa request

- Providing access to its premises and cooperating with Visa and its authorized agents in conjunction with the installation, service, repair, or inspection of Visa Extended Access or Visa Extended Access Proxy[1]

- Notifying Visa promptly of any failure of Visa Extended Access or Visa Extended Access Proxy to operate properly on its premises or the premises of its agent or independent contractor[1]

- Providing computer time and a sufficient number of qualified personnel required to ensure prompt and efficient installation and use of the V.I.P. System, BASE II, and/or other Visa applications

A Member must notify Visa of any system changes that will affect the VisaNet system and must provide Visa with a minimum of 45 calendar days' notice of changes required by the Member to services currently provided by Visa to the Member, including, but not limited to:

Visa Product and Service Rules

7 Transaction Processing

Visa Core Rules and Visa Product and Service Rules

- New Visa Extended Access of Visa Extended Access Proxy software and options

- Changes to V.I.P., BASE II, or other Visa applications

In the Canada Region: Visa owns a Visa Extended Access or Visa Extended Access Proxy server installed at a Member's location and is responsible for its acquisition, installation, and maintenance. Unless otherwise agreed by Visa, all of the following, as applicable:

- The Member may use the Visa Extended Access server only for V.I.P. System and BASE II processing.

- The Member may use the Visa Extended Access Proxy server only for Visa applications, as approved by Visa.

- Members must not share a Visa Extended Access server or Visa Extended Access Proxy server.

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing*.

[1] This does not apply to a Member using Direct Exchange (DEX).

ID# 0003332   **Edition: Apr 2020 | Last Updated: Oct 2019**

7.2.1.3   Unavailability of Visa Extended Access and Visa Extended Access Proxy

If a Member's Visa Extended Access or Visa Extended Access Proxy is expected to be unavailable, the Member must either:

- If unavailable for fewer than 5 calendar days, prepare the transmission as usual and send the Interchange to Visa as soon as the VisaNet Access Point becomes available

- If unavailable for 5 or more calendar days, send the Interchange to Visa as soon as possible

This does not apply to a Member using Direct Exchange (DEX).

ID# 0003670   **Edition: Apr 2020 | Last Updated: Oct 2019**

7.2.1.4   BIN and Acquiring Identifier Processing Requirements for Visa Extended Access – Europe Region

In the Europe Region: A Visa Extended Access server used by a Member and/or its Visa Scheme Processor must be connected to the Visa Europe Authorization Service and the Visa Europe Clearing and Settlement Service for both:

- A new request for a BIN or an Acquiring Identifier to be licensed for use in the Europe Region

- An existing BIN or Acquiring Identifier that is licensed for use in the Europe Region

This does not apply to:

- Transactions acquired under the International Airline Program by Acquirers outside of the Europe Region

- Transactions originating from an Airline or International Airline that is located outside of the Europe Region and that are acquired by an Airline Authorizing Processor

A Member that does not comply with these requirements will be subject to a non-compliance assessment.

ID# 0029595	Edition: Apr 2020	Last Updated: Oct 2019

7.2.2   Clearing Processors

7.2.2.1   Authorizing or Clearing Processor Termination or Downgrade

If an Authorizing or Clearing Processor terminates receipt or transmission of Interchange or downgrades its VisaNet processing level the Clearing Processor must both:

- Notify Visa in writing at least 3 months before the termination or effective date of the downgrade

- Be responsible for the VisaNet access charges that would have been assessed until the designated termination date, if the Clearing Processor terminates the receipt or transmission of Interchange before the designated termination date

Access and processing levels must have been in effect for at least 12 months on the designated effective date of the downgrade or termination.

ID# 0027078	Edition: Apr 2020	Last Updated: Oct 2017

7.3   Authorization

7.3.1   Authorization Routing

7.3.1.1   Account Range Table for Authorization Routing

If an Acquirer chooses to use the Account Range table provided by Visa to determine the routing of an Authorization Request, it must use the Account Range table to validate Visa Cards and must install and use the table within 6 business days of receipt.

An Acquirer must not distribute the Account Range table without the prior written consent of Visa, as specified in *Section 2.3.4.1, Disclosure of BIN Attributes.*

ID# 0008754	Edition: Apr 2020 | Last Updated: Apr 2020

7.3.1.2   Chip Transaction Routing Requirement – AP Region (Australia, Malaysia)

In the AP Region (Australia): An Acquirer must route an Authorization Request to VisaNet if a Visa Contactless or VIS-based Payment Application was selected to complete a Transaction.

In the AP Region (Malaysia): An Acquirer must ensure that Merchant choice is respected and accordingly must route an Authorization request to VisaNet if a Visa Contactless or VIS-based Payment Application was selected to complete a Transaction.

ID# 0027964	Edition: Apr 2020 | Last Updated: Apr 2018

7.3.2   Authorization Service Participation

7.3.2.1   Stand-In Processing (STIP) Transaction Approval

If Visa approves a Transaction in Stand-In Processing (STIP), both:

- Visa provides the Acquirer with an Authorization Code based on the date, time, and Payment Credential.
- The Acquirer must provide the Authorization Code to the Merchant.

ID# 0005498	Edition: Apr 2020 | Last Updated: Apr 2020

7.3.3   Member Provision of Authorization Services

7.3.3.1   Authorization Service Requirements

A Member must participate in the Card Verification Service[1] and provide Authorization services for all of its Cardholders, Merchants, or branches, 24 hours a day, 7 days a week, using one of the following methods:

- Directly, as a VisaNet Processor
- Through another VisaNet Processor, including Visa
- In the Europe Region: Through a Visa Scheme Processor
- By other means approved by Visa

An Issuer must meet the assured Transaction response standards for its Authorization Responses.

In the US Region: An Issuer or its Authorizing Processor (including Stand-In Processing) must respond to all Authorization Requests in an average time not exceeding 5 seconds during each calendar month.

[1] In the Europe Region: This does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region* it must refer to *Visa Europe Operating Regulations – Processing*.

ID# 0004381	**Edition: Apr 2020	Last Updated: Oct 2016**

7.3.3.2   Card Verification Value 2 (CVV2) – Acquirer Processing Requirements

An Acquirer must be able to both:

- Send and receive, and ensure that its Merchant is able to send and receive, responses to all Authorization Requests containing Card Verification Value 2 (CVV2) values[1]
- Correctly process all CVV2 response codes and include them in the Clearing Record

[1] In the US Region: An Acquirer must be certified.

ID# 0030124	**Edition: Apr 2020	Last Updated: Apr 2018**

7.3.3.3   Issuer Processing of Mass Transit Transactions

For a Mass Transit Transaction, an Issuer must both:

- Be able to process an Authorization Request for a Mass Transit Transaction
- Not send a Decline Response based solely on either:
  - The value of the Application Transaction Counter
  - A missing CVV2

ID# 0030051	**Edition: Apr 2020	Last Updated: Apr 2018**

7.3.3.4   Visa Delegated Authorization Processing – Europe Region

In the Europe Region: If VisaNet experiences significant degradation or becomes unavailable, Visa may notify eligible Acquirers that those Acquirers can use Visa Delegated Authorization Processing[1] for a duration of time determined by Visa.

An Acquirer must register with Visa if it wishes to be eligible to use Visa Delegated Authorization Processing.

[1] An optional program where eligible Acquirers may authorize Transactions to maintain continuity of service for Merchants

and Cardholders.

ID# 0030651	Edition: Apr 2020 | Last Updated: Oct 2019

7.3.3.5   Acquirer Unavailability Response – Europe Region

In the Europe Region: An Acquirer that is not able to submit an Authorization Request must transmit a "service unavailable now" response to an ATM or Unattended Cardholder-Activated Terminal.

ID# 0029829	Edition: Apr 2020 | Last Updated: Oct 2019

7.3.3.6   Pickup Response Prohibition for Contactless Transactions – Europe Region

In the Europe Region: An Issuer must send only an Approval Response or a Decline Response to an Authorization Request for a Contactless Transaction.

If an Acquirer receives a Pickup Response, it must process it as a Decline Response.

ID# 0029831	Edition: Apr 2020 | Last Updated: Oct 2017

7.3.4   Authorization Response Time Limits

7.3.4.1   Authorization Requests – Time Limit for Response

An Issuer must respond to an Authorization Request within the time limits specified as follows:

Table 7-1: Maximum Time Limits for Authorization Request Response

Transaction Type	AP Region, Canada Region, CEMEA Region, LAC Region, and US Region	Europe Region
POS (including PIN at POS and Unattended Cardholder-Activated Terminals where PIN is present)	10 seconds	5 seconds
ATM Cash Disbursement (MCC 6011 only)	25 seconds	5 seconds

If Visa (or, in the Europe Region, a Visa Scheme Processor) does not receive an Authorization Response from an Issuer within the specified time limit, Visa (or the Visa Scheme Processor) will respond on behalf of the Issuer, using Stand-In Processing.

ID# 0004385	Edition: Apr 2020 | Last Updated: Oct 2018

7.3.4.2   POS Transaction Timeout and Authorization Reversal

An Acquirer or a Merchant must not timeout a POS Transaction in less than 15 seconds.[1] If a Merchant receives an Approval Response after a timeout, the Merchant must submit an Authorization Reversal.

[1] In the Europe Region: This does not apply.

ID# 0030580	Edition: Apr 2020 | Last Updated: Oct 2018

7.3.5   Use of the Exception File

7.3.5.1   Exception File Updates

An Issuer must add an Account Number to an Exception File if one or more of the following applies:

- A Card was reported lost, stolen, or counterfeit and must be recovered.
- A Deposit-Only Account Number is reported as compromised.
- Authorization must always be denied to the Account Number.
- Authorization must always be granted to the Account Number.
- Issuer-defined Authorization limits apply to the Account Number.
- The Acquirer must contact the Issuer to obtain Authorization for the Account Number.

ID# 0003235	Edition: Apr 2020 | Last Updated: Apr 2020

7.3.6   Declines

7.3.6.1   Preauthorized Transaction Decline Response

Effective through 17 April 2020 Unless otherwise specified, a Recurring Transaction, an Installment Transaction, a Preauthorized Healthcare Transaction, or an Unscheduled Credential-on-File Transaction that receives a Decline Response may be resubmitted for Authorization up to 4 times

within 16 calendar days from the date of the original Decline Response, in an attempt to receive approval, only if the Decline Response code is one of the following:

- 05 (Authorization declined)
- 51 (Insufficient funds)
- 61 (Exceeds withdrawal amount limits)
- 65 (Exceeds withdrawal frequency)

Effective through 17 April 2020 If an Approval Response is not received within this timeframe, the Merchant must not deposit the Transaction.

Effective 18 April 2020 In the AP Region, CEMEA Region: Unless otherwise specified, a Recurring Transaction, an Installment Transaction, a Preauthorized Healthcare Transaction, or an Unscheduled Credential-on-File Transaction that receives a Decline Response may be resubmitted for Authorization up to 4 times within 16 calendar days from the date of the original Decline Response, in an attempt to receive approval, only if the Decline Response code is one of the following:

- 05 (Authorization declined)
- 51 (Insufficient funds)
- 61 (Exceeds withdrawal amount limits)
- 65 (Exceeds withdrawal frequency)

Effective 18 April 2020 If an Approval Response is not received within this timeframe, the Merchant must not deposit the Transaction.

ID# 0006007	Edition: Apr 2020 | Last Updated: Oct 2019

7.3.6.2   Decline Response Prohibition for Missing Card Verification Value 2 (CVV2)

An Issuer must not send a Decline Response for:

- A payment Token provisioning request[1] based solely on a missing CVV2
- A Transaction initiated with a payment Token based solely on a missing CVV2

In the Europe Region: An Issuer must not send a Decline Response based solely on a missing Card Verification Value 2 if the capture of CVV2 is prohibited or not required, as specified in *Section 10.12.2.3, Card Verification Value 2 (CVV2) Requirements – Europe Region.*

[1] Applies only to Visa Token Service participants and only to Stored Credential or Electronic Commerce enabler payment Tokens

ID# 0029985	Edition: Apr 2020 | Last Updated: Apr 2018

7.3.6.3   Resubmission following a Decline Response to a Transit Transaction

An Acquirer that has received a Decline Response to a Transaction that originates from a Mass Transit Merchant may enter that Transaction into Interchange if the following applies:

- The Merchant has received an Approval Response to a subsequent Authorization Request that included the data from the original Transaction

- The Merchant has not submitted either:

  – For a Known Fare Transaction, more than 2 Authorization Requests within 14 calendar days of the initial Decline Response

  – For a Mass Transit Transaction, following the initial Decline Response, more than the number of permitted Authorization Requests within the timeframes specified in *Section 5.9.18.2, Mass Transit Transaction Requirements*

ID# 0030046	Edition: Apr 2020	Last Updated: Apr 2018

7.3.6.4   Declined Transaction Resubmission Requirements – Canada, Europe, LAC, and US Regions

Effective 18 April 2020 In the Canada Region, Europe Region, LAC Region, US Region: Except as specified in *Section 5.9.12.1, Repayment of Debt,* and in *Section 7.3.6.3, Resubmission following a Decline Response to a Transit Transaction,* a Merchant that receives a Decline Response may resubmit the Transaction for Authorization in an attempt to receive an Approval Response up to 15 times within 30 calendar days from the date of the original Decline Response.

If an Approval Response is not received within this timeframe, the Merchant must not deposit the Transaction.

Effective 18 April 2020 in the Europe Region, LAC Region, and effective 17 April 2021 in the Canada Region, US Region A Merchant that receives a Decline Response must not resubmit the Transaction for Authorization in an attempt to receive an Approval Response if the Decline Response code is one of the following:

- 03 (Invalid merchant)

- 04 (Pickup card)

- 07 (Pickup card, special conditions)

- 12 (Invalid transaction)

- 15 (No such issuer)

- 41 (Pickup card [lost card])

- 43 (Pickup card [stolen card])

- 57 (Transaction not permitted to cardholder)

- 62 (Restricted card)

- 78 (No account)

- 93 (Transaction cannot be completed)

- R0 (Stop payment order)

- R1 (Revocation of authorization order)

- R3 (Revocation of all authorization)

ID# 0030639	Edition: Apr 2020 | Last Updated: Oct 2019

7.3.6.5   Use of Authorization Response Codes – Canada, Europe, LAC, and US Regions

Effective 18 April 2020 In the Canada Region, Europe Region, LAC Region, US Region: An Issuer must attempt to approve or partially approve an Authorization Request for any valid Payment Credential in good standing. If an Issuer is unable to approve a Transaction, it must use a Decline Response code that most accurately reflects the reason for the decline.

A VisaNet Processor must not alter an Issuer's Decline Response Code to ensure Acquirers and Merchants are able to identify the reason for a declined Transaction. Processors must be capable of supporting an Issuer's decline response mapping according to the categories below.

An Issuer that responds to an Authorization Request with a Decline Response code other than one of the following may be subject to non-compliance assessments:

Table 7-2: Permitted Authorization Response Codes

Category 1 (Issuer will not approve)	Category 2 (Issuer cannot approve at this time)	Category 3 (Data quality issues)
03 (Invalid merchant) 04 (Pickup card) 07 (Pickup card, special conditions) 12 (Invalid transaction) 15 (No such issuer) 41 (Pickup card [lost card])	19 (Re-enter transaction) 51 (Insufficient funds) 59 (Suspected fraud) 61 (Exceeds withdrawal amount limits) 65 (Exceeds withdrawal frequency)	14 (Invalid account number) 54 (Expired card) 55 (Incorrect PIN) 82 (Negative Online CAM, dCVV, iCVV, or CVV results) - N7 (Decline for CVV2 failure [Visa])

Table 7-2: Permitted Authorization Response Codes (continued)

Category 1 (Issuer will not approve)	Category 2 (Issuer cannot approve at this time)	Category 3 (Data quality issues)
• 43 (Pickup card [stolen card]) • 57 (Transaction not permitted to cardholder) • 62 (Restricted card) • 78 (No account) • 93 (Transaction cannot be completed) • R0 (Stop payment order) • R1 (Revocation of authorization order) • R3 (Revocation of all authorization)	• 75 (Allowable number of PIN-entry tries exceeded) • 86 (ATM malfunction) • 91 (Issuer or switch is inoperative) • 96 (System malfunction) • N3 (Cash service not available) • N4 (Cash request exceeds issuer limit)	• In the Europe Region: 1A (Additional customer authentication required) • In the Europe Region: 70 (PIN data required)

An Issuer must not decline an Authorization Request for a Category 1 Decline Response code and subsequently approve a resubmitted Authorization Request for the same Transaction.

ID# 0030640   Edition: Apr 2020 | Last Updated: Apr 2020

7.3.7   Authorization Reversals and Authorization Holds

7.3.7.1   Acquirer Requirement to Act on Authorization Reversal

An Acquirer that receives an Authorization Reversal from its Merchant must accept the Authorization Reversal and immediately forward it to Visa.

ID# 0005476   Edition: Apr 2020 | Last Updated: Oct 2016

7.3.8   Visa Debit with PIN – US Region

7.3.8.1   Visa Debit with PIN Transactions – Preauthorization Transactions – US Region

In the US Region: A Merchant that initiates a preauthorization request for a PIN-Authenticated Visa Debit Transaction must send a preauthorization completion message within X of the preauthorization request.

ID# 0026878   Edition: Apr 2020 | Last Updated: Oct 2014

7.3.9   Partial Authorization

7.3.9.1   Partial Authorization Service Participation – Acquirer Requirements

To participate in the Partial Authorization service, an Acquirer and its Processor must:

- Support Partial Authorization Transactions and Authorization Reversals
- Obtain systems certification from Visa to receive and transmit Visa Partial Authorization Transactions
- Ensure that its participating Merchants:
  – Include the Partial Authorization indicator in the Authorization Request
  – Submit an Authorization Reversal if the Cardholder elects not to complete the purchase
  – Submit a Clearing Transaction for no more than the amount approved in the Partial Authorization Response
  – Ensure that its participating Merchants support Partial Authorizations for all Visa Card types.

In the US Region: An Acquirer must both:

- Participate in the Partial Authorization service
- Process Partial Authorization messages for all terminals that have been programmed to participate in the Partial Authorization service

In the CEMEA Region (Kenya, Russia, Serbia, Ukraine): An Acquirer must both:

- Participate in the Partial Authorization service for domestic POS Transactions with Cash-Back
- Process Partial Authorization messages for all terminals that have been programmed to participate in the Partial Authorization service

ID# 0002515   Edition: Apr 2020 | Last Updated: Apr 2019

7.3.9.2   Automated Fuel Dispenser Partial Authorization Merchant Requirements

An Automated Fuel Dispenser Merchant that participates in the Partial Authorization service must both:

- Include the Partial Authorization indicator in the Authorization Request or Status Check Authorization (where permitted)

- For a Transaction where the full Transaction amount is included in the Authorization Request, submit a Clearing Transaction for no more than the amount approved in the Partial Authorization Response

In the Europe Region: An Automated Fuel Dispenser Merchant must participate in the Partial Authorization service.

ID# 0002520	Edition: Apr 2020 | Last Updated: Oct 2016

7.3.9.3   Partial Authorization Service Acquirer Participation – Canada Region

In the Canada Region: An Acquirer and its VisaNet Processor must both:

- Receive and transmit Partial Authorization Transactions and Authorization Reversals for the following MCCs:
  - 4121 (Taxicabs and Limousines)
  - 4812 (Telecommunication Equipment and Telephone Sales)
  - 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls Through Use of Magnetic Stripe Reading Telephones, and Fax Services)
  - 4816 (Computer Network/Information Services)
  - 5200 (Home Supply Warehouse Stores)
  - 5310 (Discount Stores)
  - 5311 (Department Stores)
  - 5331 (Variety Stores)
  - 5411 (Grocery Stores and Supermarkets)
  - 5499 (Miscellaneous Food Stores – Convenience Stores and Specialty Markets)
  - 5541 (Service Stations [With or Without Ancillary Services])
  - 5542 (Automated Fuel Dispensers)
  - 5621 (Women's Ready-To-Wear Stores)

- 5631 (Women's Accessory and Specialty Shops)
- 5641 (Children's and Infants' Wear Stores)
- 5651 (Family Clothing Stores)
- 5661 (Shoe Stores)
- 5691 (Men's and Women's Clothing Stores)
- 5732 (Electronics Stores)
- 5734 (Computer Software Stores)
- 5735 (Record Stores)
- 5812 (Eating Places and Restaurants)
- 5814 (Fast Food Restaurants)
- 5912 (Drug Stores and Pharmacies)
- 5921 (Package Stores – Beer, Wine, and Liquor)
- 5941 (Sporting Goods Stores)
- 5942 (Book Stores)
- 5945 (Hobby, Toy, and Game Shops)
- 5947 (Gift, Card, Novelty and Souvenir Shops)
- 5977 (Cosmetic Stores)
- 5999 (Miscellaneous and Specialty Retail Stores)
- 7230 (Beauty and Barber Shops)
- 7298 (Health and Beauty Spas)
- 7399 (Business Services [Not Elsewhere Classified])
- 8999 (Professional Services [Not Elsewhere Classified])
- 9399 (Government Services [Not Elsewhere Classified])
- Obtain systems certification from Visa for Partial Authorization Transaction processing, as follows:
  - Standalone POS deployed on or after 17 April 2017
  - Integrated POS deployed on or after 16 April 2017
  - **Effective 13 October 2022** All standalone POS
  - **Effective 13 October 2022** All integrated POS

ID# 0029230   Edition: Apr 2020 | Last Updated: Oct 2016

7.3.9.4   Partial Authorization Service – Issuer Requirements

To participate in the Partial Authorization service, an Issuer and its Processor must support Partial Authorizations and Authorization Reversals.

| ID# 0029818 | Edition: Apr 2020 | Last Updated: Oct 2016 |

7.3.11   Account Verification – Europe Region

7.3.11.1   Account Verification Processing – Europe Region

In the Europe Region: An Issuer must be able to respond to Account Verification requests by sending a response code that indicates either:

- No reason to decline
- Non-approval

An Acquirer must do all of the following:

- Be able to transmit the Account Verification request to the Issuer
- Be able to receive the response from the Issuer for that Account Verification request
- Ensure that its Merchants use Account Verification to validate a Cardholder account. This does not apply to Automated Fuel Dispensers.

| ID# 0029668 | Edition: Apr 2020 | Last Updated: Oct 2016 |

7.3.12   Member Reporting Requirements – Europe Region

7.3.12.1   Member Reporting Requirements – Europe Region

In the Europe Region: A Member that processes Transactions must submit to Visa a daily transmission file detailing those Transactions including Authorization Responses that are Approval Responses or Decline Responses.

A Member must not report transactions where a Cardholder has chosen to use a payment brand or application that is not part of the Visa Europe Scheme.

An Issuer must report a Dispute within 15 calendar days of the Processing Date of the Dispute.

An Acquirer must report a Dispute Response or pre-Arbitration within 15 calendar days of the Processing Date of the Dispute Response or pre-Arbitration.

ID# 0029678	Edition: Apr 2020 | Last Updated: Apr 2018

7.4 Processing of Specific Transaction Types

7.4.1 Account Funding Transactions

7.4.1.1 Account Funding Transaction Requirements

Effective 18 April 2020 An Account Funding Transaction must be used for the following:

- Reloading Prepaid Cards
- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: In the Card-Absent Environment, all of the following:
  – Funding person-to-person money transfers, including account-to-account money transfers
  – Funding disbursements of funds from Visa Corporate Cards, Visa Business Debit Cards, or Visa Business Check Cards (for example: payroll)
  – Pre-funding stored value digital wallets (except single-Merchant digital wallets) that will then be used for money transfers or purchases, and Staged Digital Wallets

An Account Funding Transaction must do all of the following:

- Be processed with an Account Funding Transaction indicator and the correct business application identifier (BAI) in the Authorization Request and Clearing Record
- Not represent any of the following:
  – Payment for goods or services (except Visa Scan to Pay program Transactions)
  – Funding of a Merchant account
  – Debt repayment
- **Effective 18 April 2020** Comply with the *Account Funding Transaction (AFT): Processing Guide*

ID# 0002890	Edition: Apr 2020 | Last Updated: Apr 2020

7.4.2 Manual Cash Disbursements

7.4.2.1 Manual Cash Disbursement Transaction Currency

The Transaction Currency for a Manual Cash Disbursement must be all of the following:

- Currency dispensed
- Currency in the Authorization Request
- Currency presented into Interchange

ID# 0006862	Edition: Apr 2020	Last Updated: Oct 2017

7.4.2.2   Issuer Minimum Manual Cash Disbursement Amount

An Issuer must not establish a minimum Manual Cash Disbursement amount.

ID# 0006858	Edition: Apr 2020	Last Updated: Apr 2015

7.4.3   Automated Fuel Dispenser Transactions

7.4.3.1   Automated Fuel Dispenser Real-Time Clearing Transaction Processing

An Automated Fuel Dispenser Merchant that participates in Real-Time Clearing must also participate in Partial Authorization.

A Real-Time Clearing Transaction must identify the preauthorization time limit in field 63.2 of the Authorization message.

The Completion Message must be for an amount equal to or less than the authorized amount, including partial approvals.

ID# 0007391	Edition: Apr 2020	Last Updated: Oct 2017

7.4.3.2   Automated Fuel Dispenser Transaction Issuer Requirements – Europe Region

In the Europe Region: An Issuer must do all of the following:

- Be able to process Automated Fuel Dispenser (AFD) Transactions with a maximum amount (no more than EUR 150 [or local currency equivalent], unless explicitly preselected by the Cardholder) included in the Authorization Request amount
- Support the receipt of an Acquirer confirmation advice in real time
- Immediately act upon the Acquirer confirmation advice and adjust the Cardholder's available funds
- Support Partial Authorizations

ID# 0029982	Edition: Apr 2020	Last Updated: Apr 2018

7.4.4   Bill Payment Transactions

7.4.4.1   ATM Bill Payments – LAC Region (Brazil)

In the LAC Region (Brazil): An Acquirer must not use Deferred Settlement when processing a domestic Bill Payment Transaction at an ATM.

ID# 0029526	Edition: Apr 2020 | Last Updated: Apr 2017

7.4.4.2   Bill Payment Transaction Data – US Region

In the US Region: An Acquirer must identify a Bill Payment Transaction in the Authorization Request and Clearing Record.

ID# 0008913	Edition: Apr 2020 | Last Updated: Oct 2014

7.4.6   Online Gambling Transactions

7.4.6.1   Quasi-Cash/Online Gambling Transaction Indicator

A Quasi-Cash Transaction must be processed with a Quasi-Cash Transaction indicator in the Authorization Request and Clearing Record.

In the CEMEA Region (South Africa): This does not apply.

ID# 0002886	Edition: Apr 2020 | Last Updated: Oct 2017

7.4.7   Commercial Payables Transactions

7.4.7.1   Authorization Request and Settlement Amount Match

Visa will return a Commercial Payables Transaction to the Acquirer for resubmission if the amount in the Clearing Record does not match the amount in the Authorization Request and all of the following conditions apply:

- Card is a Visa Purchasing or Visa Fleet Card
- Issuer has enrolled to participate in the Authorization and Settlement Match service
- The Visa Purchasing Card BIN or Account Range (including Visa Fleet Card BIN or Account Range) is enrolled in the Authorization and Settlement Match service
- Transaction occurs in a Card-Absent Environment

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing*.

ID# 0026827	Edition: Apr 2020 | Last Updated: Apr 2019

7.4.8   Card-Absent Environment Transactions – AP Region

7.4.8.1   Mail/Phone Order Expiration Date in Authorizations – AP Region

In the AP Region: An Authorization Request for a Mail/Phone Order Transaction must include the Card expiration date.

This does not apply to Recurring Transactions, which do not require an expiration date in the Authorization Request.

ID# 0005333	Edition: Apr 2020 | Last Updated: Oct 2014

7.4.9   Visa Purchasing Card Transactions

7.4.9.1   Visa Purchasing Card Transaction Data

An Acquirer that accepts a Visa Purchasing Card Transaction must provide the Issuer with any Cardholder reference data or other relevant Transaction information supplied by a Merchant.

ID# 0008893	Edition: Apr 2020 | Last Updated: Oct 2014

7.4.10   Visa Fleet Card Transactions

7.4.10.1   Visa Fleet Card – Enhanced Data

An Acquirer that contracts with a Merchant to accept a Visa Fleet Card must provide the Issuer or the Issuer's agent with the Enhanced Data if provided by its Merchant in the Authorization and Clearing Record.

ID# 0008894	Edition: Apr 2020 | Last Updated: Oct 2015

7.4.10.2   Visa Fleet Card Enhanced Data Requirements – US Region

In the US Region: A Merchant that accepts a Visa Fleet Card must provide Enhanced Data for Visa Fleet Card Transactions classified with any of the following MCCs:

- 4468 (Marinas, Marine Service, and Supplies)

- 5499 (Miscellaneous Food Stores – Convenience Stores and Specialty Markets)

- 5541 (Service Stations)

- 5542 (Automated Fuel Dispensers)

- 5983 (Fuel Dealers – Fuel Oil, Wood Coal, and Liquefied Petroleum)

An Acquirer that processes Visa Fleet Card Transactions must provide both Cardholder-supplied data and supplemental Transaction data for these Transactions.

ID# 0027524	Edition: Apr 2020 | Last Updated: Apr 2015

7.4.11   Visa Commercial Card Transactions

7.4.11.1   Visa Commercial Card Data Requirements – Europe Region

In the Europe Region: If a Merchant provides Enhanced Data in the Authorization Request and Clearing Record, its Acquirer must provide the Enhanced Data to the Issuer.

An Acquirer must provide the following data to the Issuer:

- All tax details, as agreed by Visa and the national fiscal authorities

- Unique customer reference data, if supplied by the Client Organization

An Acquirer whose Merchants provide Enhanced Data for Visa Purchasing Card Transactions must provide to Visa contact details for the participating Merchant Outlets every 6 months or as determined by Visa.

ID# 0029673	Edition: Apr 2020 | Last Updated: Oct 2017

7.4.11.2   Visa Purchasing Card Enhanced Data Requirements – Europe Region

In the Europe Region: A Visa Purchasing Card Issuer must both:

- Receive level II and level III Enhanced Data from Merchants

- Either:

  – Use an enhanced data BIN from a specified Visa Purchasing Card BIN range

  – Designate an Account Range of an existing Visa Purchasing Card BIN

ID# 0029630	Edition: Apr 2020 | Last Updated: Oct 2019

7.4.11.3   Visa Business Card and Visa Corporate Card Enhanced Data Processing – Europe Region

In the Europe Region: A Visa Business Card Issuer and Visa Corporate Card Issuer may configure BINs or Account Ranges within those BINs to receive and process Enhanced Data for management information purposes.

ID# 0029631   **Edition: Apr 2020 | Last Updated: Oct 2019**

7.4.11.4   Enhanced Data Processing Requirements – US Region

In the US Region: A Visa Purchasing Card Issuer that chooses to receive Level II Enhanced Data and Level III Enhanced Data from a Merchant must either:

- Designate an Account Range of the enhanced data Visa Purchasing Card BIN
- Use an enhanced data BIN from a specified Visa Purchasing Card BIN range

ID# 0004156   **Edition: Apr 2020 | Last Updated: Oct 2019**

7.4.12   Visa Drive Card Transactions – Europe Region

7.4.12.1   Cash Disbursements on Visa Drive Cards – Europe Region

In the Europe Region: Cash Disbursements are not permitted on Visa Drive Cards that are "standard" Cards or "extra" Cards.

Cash Disbursements are permitted on Visa Drive Cards that are "open" Cards.

ID# 0029810   **Edition: Apr 2020 | Last Updated: Oct 2016**

7.4.12.2   Quasi-Cash Transactions on Visa Drive Cards – Europe Region

In the Europe Region: Quasi-Cash Transactions are not permitted on Visa Drive Cards that are "standard" Cards or "extra" Cards.

Quasi-Cash Transactions are permitted on Visa Drive Cards that are "open" Cards.

ID# 0029835   **Edition: Apr 2020 | Last Updated: Oct 2016**

7.4.13   In-Transit Transactions – Europe Region

7.4.13.1   In-Transit Gambling Merchant Requirements – Europe Region

In the Europe Region: A Gambling Merchant must ensure that an In-Transit Transaction for the purchase of gambling is processed as a Quasi-Cash Transaction.

ID# 0029834	Edition: Apr 2020 | Last Updated: Oct 2016

7.4.14   Authorization Request Content – Europe Region (United Kingdom)

7.4.14.1   Authorization Request Content for MCC 6012 – Europe Region (United Kingdom)

In the Europe Region (United Kingdom): An Acquirer that processes a Transaction in a Card-Absent Environment using MCC 6012 (Financial Institutions – Merchandise, Services, and Debt Repayment) must include in the Authorization Request all of the following data elements for the recipient account holder:

- Date of birth
- Account number (either partially masked or up to 10 characters)
- Partial postcode
- Last name

The Issuer that receives the Authorization Request must check the data elements against its own data about the recipient of the payment.

ID# 0030058	Edition: Apr 2020 | Last Updated: Oct 2017

7.5   Clearing

7.5.1   File Processing

7.5.1.1   Duplicate Interchange File Requirements

A Member must generate a duplicate Interchange File before transmitting Interchange to Visa and retain this file for 15 calendar days after the Settlement Date.

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing.*

ID# 0003372	Edition: Apr 2020 | Last Updated: Oct 2016

7.5.2   Currency Conversion

7.5.2.1   Currency Conversion

Visa converts the Transaction Currency to the Issuer's or Acquirer's Settlement Currency using the Currency Conversion Rate.

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing.*

ID# 0003298	Edition: Apr 2020 | Last Updated: Oct 2016

7.5.3   PIN-Authenticated Visa Debit Adjustments – US Region

7.5.3.1   PIN-Authenticated Visa Debit Transaction Adjustments – US Region

In the US Region: If an Acquirer processes an Adjustment to a PIN-Authenticated Visa Debit Transaction to correct a Merchant or Acquirer processing error that causes an out-of-balance situation, it must both:

- Process the Adjustment within 45 calendar days of the purchase date of the original Transaction
- Process the Adjustment for the correct Transaction amount

An Acquirer may process a first Presentment as an Original Adjustment when all of the following apply:

- Original Transaction resulted from a PIN-Authenticated Visa Debit Transaction
- Connection between the Merchant and its Authorizing Processor was inoperable
- Merchant completed the Transaction without obtaining an Authorization

An Acquirer must not process an Original Adjustment if the original Transaction received a Decline Response.

The Acquirer must not process an Adjustment subsequent to a Dispute.

ID# 0026510   Edition: Apr 2020 | Last Updated: Apr 2018

7.5.4 Reversals – US Region

7.5.4.1 Correction of Duplicate or Erroneous Clearing Transaction Data

Effective through 16 April 2021 In the US Region: If a Clearing Processor that cleared Interchange through VisaNet detects duplicate or erroneous data before sending it to Visa, the Clearing Processor must correct the data before transmission.

Effective 17 April 2021 If a Clearing Processor that cleared Interchange through VisaNet detects duplicate or erroneous data before sending it to Visa, the Clearing Processor must correct the data before transmission.

If incorrect data has already been transmitted, a clearing reversal may be initiated by either the Clearing Processor that originated the duplicate or erroneous transmission or by Visa.

The Clearing Processor must use a clearing reversal to correct either:

- Inadvertent processing errors (for example: duplicate processing)
- Individual Transactions that were transmitted more than once or contain erroneous data

To reverse a duplicate or erroneous Interchange transmission, the Clearing Processor must do all of the following:

- Immediately notify Visa of any duplicate or erroneous data transmitted, including any of the following:
  – An entire day's Interchange duplication
  – Batches of previously transmitted Interchange
  – Batches captured more than once on the same outgoing Interchange File
  – Batches, files, or individual transactions with erroneous data
- Replace the Transaction codes of the duplicate Transactions with the appropriate Clearing Reversal codes
- Not change any other information in the duplicate Transactions
- Send the corrected file on the next transmission day

ID# 0008882   Edition: Apr 2020 | Last Updated: Apr 2020

7.5.5   Data Requirements

7.5.5.1   Interchange Data Element Requirements

An Acquirer that sends Interchange through BASE II must use the data elements listed in the applicable VisaNet documentation.

ID# 0005521	Edition: Apr 2020	Last Updated: Apr 2018

7.5.5.2   Prepaid Card Purchase Transaction Data

A Transaction representing the purchase of a Prepaid Card must be processed as a retail purchase and include a Prepaid Card indicator in the Transaction record.

ID# 0002516	Edition: Apr 2020	Last Updated: Apr 2020

7.5.5.3   Visa Commercial Card and Prepaid Card Data Requirements – LAC Region (Brazil)

In the LAC Region (Brazil): An Acquirer must ensure that the Clearing Record for a Transaction completed with a Visa Commercial Card or a Prepaid Card of a government program includes the Merchant legal name and Merchant tax identification number.

ID# 0027384	Edition: Apr 2020	Last Updated: Apr 2020

7.6   Online Financial and Deferred Clearing

7.6.1   Online Financial and Deferred Clearing Requirements

7.6.1.1   Online Financial Transaction Processing Requirements

An Online Financial Transaction Authorization Request for a Visa or Visa Electron Transaction must originate at an ATM or an Acceptance Device and include both the:

- **Effective through 19 July 2019** Entire unaltered contents of track 1 or track 2 of the Magnetic Stripe, the Magnetic-Stripe Image on the Chip, or the track 2 equivalent data in a QR code
- **Effective 20 July 2019** Entire unaltered contents of track 1 or track 2 of the Magnetic Stripe, the Magnetic-Stripe Image on the Chip, or in the AP Region, the track 2 equivalent data in a QR code
- Final amount of the Transaction

An Online Financial Transaction that is a purchase Transaction may only be key-entered either:

- In a Card-Absent Environment

- If the Magnetic Stripe cannot be read. This does not apply to a Visa Electron Transaction, which may not be key-entered.

An Acquirer must process a Clearing Reversal for an Online Financial or Deferred Clearing Transaction if either the:

- Acquirer or Merchant sent an Authorization Request and did not receive an Authorization Response

- Transaction is subsequently voided or cancelled

| ID# 0008863 | Edition: Apr 2020 \| Last Updated: Apr 2020 |

7.7   Transaction Processing Time Limits and Dates

7.7.1   Processing Time Limits

7.7.1.1   Acquirer Processing Timeframes

An Acquirer must process Transactions within the following timeframes:

Table 7-3: Acquirer Processing Timeframe Requirements

Transaction Type	Maximum Processing Timeframe
Visa Electron and ATM[1]	- Within 5 calendar days of the Transaction Date - **Effective 1 November 2019** In the AP Region (India): For a Domestic Transaction, within 4 calendar days of the Transaction Date
Visa Prepaid Load Service In the US Region: Visa ReadyLink	Within 2^1 calendar days of the Transaction Date
Merchandise Returns and Credits	Within 5^2 calendar days of the Transaction Date
All Other Transactions	- Within 8^2 calendar days of the Transaction Date - **Effective 1 November 2019** In the AP Region (India): For a Domestic Transaction, within 4 calendar days of the Transaction Date - In the AP Region (Japan): Within 30 calendar days of the

Table 7-3: Acquirer Processing Timeframe Requirements (continued)

Transaction Type	Maximum Processing Timeframe
	Transaction Date • In the AP Region (Malaysia): For domestic Automated Fuel Dispenser Transactions, within 2 local business days of the Transaction Date • In the Europe Region: For intraregional Contactless Transactions (except Mass Transit Transactions), within 2 calendar days of the Transaction Date
[1] In the US Region: ATM Transactions, PIN-authenticated Visa Debit Transactions, and Visa ReadyLink Transactions must be processed through the Single Message System. [2] In the US Region: Additional requirements for Transaction processing time limits apply to Custom Payment Service Programs.	

The Processing Date and Transaction Date are each counted as one day.

7.7.1.2   Transaction Date Limits

For a Deferred Payment Transaction, the Transaction Date must be the billing date, which must be no later than 90 calendar days from the initial shipment date.

For a Transaction involving goods that are shipped (except for an Advance Payment), the Transaction Date must be on or after the date on which the goods are shipped.

For a Mass Transit Transaction, the Transaction Date must be the last day of travel.

In the US Region: For a Preauthorized Health Care Transaction, the Transaction Date must be the date on which the Health Care Merchant receives a notice of adjudication from the Cardholder's insurance company.

7.8   Settlement

7.8.2   National Net Settlement Service (NNSS) Requirements

7.8.2.1   Use of National Net Settlement Service (NNSS)

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Member must enroll all of its BINs in the National Net Settlement Service (NNSS), if available in its country. This does not apply to:

- A Visa-approved program for which the Settlement Currency or Billing Currency is not the local currency

- In the AP Region (Japan): A Member that is not a Principal-Type Member

- In the Canada Region: A Member that has a Private Agreement for the Settlement of Domestic Transactions

A Member that participates in an NNSS must both:

- Use the NNSS to process and settle all qualifying Domestic Transactions that were processed through VisaNet in local currency

- Comply with the applicable NNSS operating procedures

In the LAC Region (Aruba, Brazil, Curacao, Sint Maarten, Venezuela): An Acquirer must process all Domestic Transactions from an Acquiring Identifier participating in the NNSS in local currency.

Visa may suspend the operation of an NNSS in an emergency. Upon suspension of an NNSS, Visa may redirect Domestic Transactions into the International Settlement Service and collect the full amount owed from a Member's nominated Settlement account or Settlement Bank.

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing.*

ID# 0029856	Edition: Apr 2020 | Last Updated: Oct 2019

7.8.3   Settlement Requirements – AP Region

7.8.3.2   Member Responsibility for Settlement Obligations – AP Region

In the AP Region: A Member is responsible for all Settlement obligations owed to Visa by any entity or subsidiary owned or controlled by the Member, even if the entity is legally independent

of the Member. Visa may offset any amount owed to Visa by the entity or subsidiary against the Member accounts, Branches, or other owned or controlled entity worldwide.

ID# 0005423 Edition: Apr 2020 | Last Updated: Oct 2014

7.8.4   Settlement Requirements – Europe Region

7.8.4.3   Visa Responsibility for Settlement – Europe Region

In the Europe Region: Without prejudice to any Issuer's or Acquirer's obligations in *Section X*, Visa will be responsible on the terms and subject to the conditions of this section to satisfy payment obligations that have arisen in relation to:

- Transactions that are Visa Transactions. For a co-badged Card, where a Cardholder chooses to initiate a transaction through a payment scheme that is not Visa, that transaction is not a Visa Transaction.
- Visa Transactions, where such Visa Transactions were reported to Visa within 24 hours of the Transaction Date
- Visa Transactions, where such Visa Transactions meet Visa data quality standards, in accordance with all applicable technical specifications
- A Visa Scheme Processor, and the Member has satisfied its obligations in relation to that Visa Scheme Processor as specified in the Visa Rules
- A Settlement failure, where such Settlement failure was reported to Visa within 24 hours of the date that any given Member is owed funds
- Visa Transactions that were accepted in accordance with the Rules

For the avoidance of doubt, Visa reserves the right to adjust its payment obligation to a Member, where that Member has reported to Visa inconsistent Transaction volumes over the preceding 18 months.

ID# 0029572 Edition: Apr 2020 | Last Updated: Oct 2016

7.8.4.11   Indemnification – Europe Region

In the Europe Region: Each Issuer and each Acquirer Indemnifies Visa for and against Claims and Liabilities that may be asserted against or incurred by Visa arising out of or in connection with a failure (or any allegation made in good faith of a failure) by such Issuer or such Acquirer (or any entity acting on its behalf or under its direction or control) to discharge its payment obligations when due and/or to comply with, be bound by and perform all obligations and duties imposed upon it pursuant to the Rules, including without limitation any failure to put Visa in funds for the

purposes of Settlement and/or any failure to satisfy any request made pursuant to the Rules. If requested by Visa, the relevant Issuer or Acquirer will provide cash or other collateral acceptable to Visa in such amounts and on such terms as Visa may deem appropriate to cover Visa against Visa's estimate of any future Claims and Liabilities for which such Issuer or Acquirer may be liable, including, without limitation, to fund Visa's relevant legal expenses.

ID# 0029580	Edition: Apr 2020 | Last Updated: Apr 2018

7.8.4.12   Member Liability – Europe Region

A Europe Group Member is jointly and severally liable for the obligations of each of its Group Issuers/Acquirers under *Section 7.8.4.11, Indemnification – Europe Region.*

A Europe Principal Member is jointly and severally liable for the obligations of each of its Sponsored Issuers/Acquirers under *Section 7.8.4.11, Indemnification – Europe Region.*

In the Europe Region: Visa will seek Indemnification or other recovery for Claims or Liabilities:

- First, from the Issuer or Acquirer that Visa deems liable under *Section 7.8.4.11, Indemnification – Europe Region*
- Second, from any Group Member and/or Principal Member that Visa deems liable under this section

Nothing in this section:

- Creates a duty of care from Visa to any entity
- Obliges Visa:
  – To institute proceedings or exhaust its rights to recover Indemnifiable Liabilities from any entity before claiming against another entity in the order of priority
  – To pro-rate or apportion its claims between different entities
- Renders an Issuer's/Acquirer's obligation to pay Visa under this section conditional upon any other entity's payment or agreement to pay

ID# 0029581	Edition: Apr 2020 | Last Updated: Apr 2018

7.8.4.16   Estimating Settlement – Europe Region

In the Europe Region: Visa reserves the right to require that Members settle on estimates provided by Visa if Clearing and Settlement is delayed.

ID# 0030062	Edition: Apr 2020 | Last Updated: Oct 2017

7.8.4.17   Loss Sharing – Europe Region

In the Europe Region: If Visa incurs a loss following the failure of a Member to satisfy its payment obligations and Visa determines, in its absolute discretion, that the loss will not be recovered in a timely manner, as specified in *Section 7.8.4.12, Member Liability – Europe Region,* Visa may apportion some or all of the loss among Principal Members.

Visa will assess a Member's Loss Share Contribution[1] according to a Loss Share Contribution calculation, available on Visa Online and as amended from time to time. Visa reserves the right to adjust the amount claimed from a Member on such basis that Visa considers equitable in the circumstances.

Visa will collect the required amount, through its settlement systems, within 120 calendar days of the loss, as either:

- A series of installments, with each installment representing no more than 5% of the total amount owed by the Member

- The total amount

If the amount collected by Visa is later determined to be more than the amount required for that Member's share, Visa will return the excess amount to the Member within 120 calendar days of the verification of the excess amount.

[1]   A financial contribution paid by a Principal Member to Visa, following the failure of any given Member to satisfy its payment obligation.

ID# 0030096	Edition: Apr 2020 | Last Updated: Apr 2018

7.8.6   Settlement Requirements – US Region

7.8.6.4   Member Responsibility for Settlement Financial Obligations – US Region

In the US Region: An Issuer is responsible for any amount due for all Transaction Receipts bearing its BIN and resulting from a Merchant or another Member honoring a valid, properly presented Card.

ID# 0005710	Edition: Apr 2020 | Last Updated: Oct 2019

7.8.6.5   Prohibition against Transferring Obligation to Pay – US Region

In the US Region: An Acquirer must not waive, release, abrogate, or otherwise assign to a non-Member its obligation to guarantee and ensure payment for all Transactions in which its Merchant honored a valid Visa Card properly presented for payment.

ID# 0005146	Edition: Apr 2020 | Last Updated: Oct 2014

7.8.6.6   Requirement for Funds Held by Acquirer – US Region

In the US Region: An Acquirer holding funds as security to ensure proper Merchant performance must hold the funds in an account in the Merchant's name.

ID# 0005147	Edition: Apr 2020 | Last Updated: Oct 2014

7.8.7   Member Readiness for Settlement

7.8.7.1   Member Readiness for Settlement

Upon submission of a Clearing Record to VisaNet, a Member must be ready to settle the Transaction within the timeframe specified by Visa for the applicable settlement service and Settlement Currency.

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing*.

ID# 0029031	Edition: Apr 2020 | Last Updated: Oct 2016

7.9   System Use – Europe Region

7.9.1   Default Infrastructure – Europe Region

7.9.1.1   Default Infrastructure Nomination – Europe Region

In the Europe Region: Visa reserves the right to nominate a Default Infrastructure, which is the processor of last resort that a Member should use when its processing infrastructure has failed or is otherwise unavailable.

ID# 0029582	Edition: Apr 2020 | Last Updated: Oct 2016

7.10   Authorization and Clearing Transaction Content

7.10.1   Transaction Message Content

7.10.1.1   Use of Payment Account Reference

An Acquirer must be capable of processing a Transaction containing a Payment Account Reference (PAR) and delivering the PAR to a Merchant.

A domestic switch or any other form of processor must be capable of transmitting a PAR when provided by an Issuer, Acquirer, or Token Requestor.

ID# 0030038	Edition: Apr 2020	Last Updated: Oct 2018

7.10.2   Stop Payment Service

7.10.2.1   Use of Payment Stop Instructions – Europe Region

Effective through 16 August 2020 In the Europe Region: An Issuer may place a stop instruction against an Authorization Request or a Clearing Record only if it complies with all of the following:

- Obtains a stop instruction request from the Cardholder
- Ensures that the stop instruction is only placed against a Recurring Transaction, an Installment Transaction, or an Unscheduled Credential-on-File Transaction
- Correctly identifies the stop instruction

ID# 0029681	Edition: Apr 2020	Last Updated: Apr 2020

7.10.2.2   Stop Payment Service Requirements

Effective 17 August 2020 in the Europe Region, and effective 19 October 2020 in the AP Region, Canada Region, CEMEA Region, LAC Region, US Region An Issuer that participates in the Stop Payment Service must do all of the following:

- Obtain a stop payment instruction request from the Cardholder
- Correctly specify the type of stop payment instruction
- Provide complete and accurate information pertaining to the stop payment instruction
- Keep stop payment instruction information current in the Stop Payment Service

Effective 17 August 2020 in the Europe Region, and effective 19 October 2020 in the AP Region, Canada Region, CEMEA Region, LAC Region, US Region A Member must not disclose information associated with the Stop Payment Service other than data relating to the Member's own Cardholder and/or Merchant to any other party unless otherwise authorized by Visa.

ID# 0030698   Edition: Apr 2020 | Last Updated: New

7.11   Strong Customer Authentication – Europe Region

7.11.1   Strong Customer Authentication – General Requirements

7.11.1.1   General Requirements for Strong Customer Authentication – Europe Region

In the Europe Region: A Member must comply with both the *Visa Delegated Authentication Implementation Guide*, *Visa Trusted Listing Implementation Guide*, and *PSD2 Strong Customer Authentication for Remote Electronic Transactions – European Economic Area*. A Member acknowledges that, regardless of any participation in the Delegated Authentication Program or Trusted Listing Program, all applicable regulatory obligations relating to the provision of strong customer authentication remain with that Member.

In the Europe Region: A Member must ensure that Electronic Commerce Transactions initiated on Cards issued in the European Economic Area (EEA) and United Kingdom are subject to strong customer authentication in line with the Payment Services Directive 2 (EU) 2015/2366.

ID# 0030622   Edition: Apr 2020 | Last Updated: Apr 2020

7.11.2   Delegated Authentication Program – Europe Region

7.11.2.1   Delegated Authentication Program Issuer Requirements – Europe Region

In the Europe Region: All Issuers in the European Economic Area (EEA) and United Kingdom will be enrolled, by Visa to participate in the Delegated Authentication Program. An Issuer may, at any time, opt out of participating in the program. By participating in the program, an Issuer agrees to delegate its provision of strong customer authentication to an Acquirer or Token Requestor. In turn, the Acquirer will sub-delegate to an enrolled Strong Customer Authentication Delegate, in accordance with the Delegated Authentication Program.

Visa will update Issuers, from time to time, on Strong Customer Authentication Delegates that have been enrolled in the Delegated Authentication Program and their relevant Acquirers. An Issuer is responsible for ensuring that its regulator, as applicable, is notified of the Issuer's Strong Customer Authentication Delegates and their relevant Acquirers.

Where a Transaction has been presented as authenticated and carries the delegated authority flag, an Issuer must not request additional authentication of the Transaction unless there is an immediate fraud threat. An Issuer must not systematically decline a Transaction that carries a delegated authority flag.

ID# 0030619	Edition: Apr 2020	Last Updated: Apr 2019

7.11.2.2   Delegated Authentication Program Acquirer Requirements – Europe Region

In the Europe Region: An Acquirer in the European Economic Area (EEA) and United Kingdom may enroll an entity in the Delegated Authentication Program. A participating Acquirer may only enroll a Strong Customer Authentication Delegate that both:

- Meets the necessary fraud level requirements, both initial and on-going, as specified in the *Visa Delegated Authentication Implementation Guide*
- Provides at least two-factor authentication in a manner that meets all applicable regulatory requirements for the provision of strong customer authentication to Cardholders

Visa may refuse the enrollment of an entity by an Acquirer into the Delegated Authentication Program if Visa determines that the entity introduces unnecessary risk into the payments system.

ID# 0030617	Edition: Apr 2020	Last Updated: Apr 2019

7.11.2.3   Delegated Authentication Program Enrollment – Europe Region

In the Europe Region: To enroll an entity in the Delegated Authentication Program an Acquirer must provide to Visa a completed Merchant Readiness Questionnaire for each potential Strong Customer Authentication Delegate. Visa will confirm when a Strong Customer Delegate has been enrolled. An Acquirer must not treat an entity as a Strong Customer Authentication Delegate in advance of Visa's confirmation.

Visa may share information about Strong Customer Authentication Delegates, provided by the Acquirer, and details of the relevant Acquirer, to all applicable Issuers and Regulators.

Visa may, at any time, terminate or suspend the enrollment of a Strong Customer Authentication Delegate in the Delegated Authentication Program, including where it determines that the Strong Customer Authentication Delegate no longer meets the requirements of the program or introduces unnecessary risk into the payments system.

Visa will update Acquirers, from time to time, on Token Requestors that have been enrolled, by Visa, in the Delegated Authentication Program.

ID# 0030618	Edition: Apr 2020	Last Updated: Apr 2019

7.11.3   Trusted Listing Program – Europe Region

7.11.3.1   Trusted Listing Program Issuer Requirements – Europe Region

In the Europe Region: An Issuer that supports trusted listing must provide Visa with BIN or Account Ranges for all Cardholders that are eligible to join the Trusted Listing Program.

An Issuer must both:

- Obtain clear instruction, from a Cardholder, to list a Trusted Beneficiary
- Remove a Trusted Beneficiary, if a Cardholder instructs the Issuer that they no longer consider that entity as trusted

Strong customer authentication must be completed at the point of adding or removing a Trusted Beneficiary.

An Issuer must not systematically decline a Transaction that carries a trusted listing indicator.

An Issuer acknowledges that, regardless of any participation in the Trusted Listing Program, all applicable regulatory obligations relating to the provision of strong customer authentication remain with the Issuer.

ID# 0030633	Edition: Apr 2020 | Last Updated: Apr 2019

7.11.3.2   Trusted Listing Program Acquirer Requirements – Europe Region

In the Europe Region: An Acquirer must register with Visa an Electronic Commerce Merchant that chooses to act as a Trusted Beneficiary.

A Trusted Beneficiary must meet fraud level requirements, both initial and ongoing, as specified in the *Visa Trusted Listing Implementation Guide*.

Visa may, at any time, terminate or suspend a Trusted Beneficiary from the Trusted Listing Program, including where it determines that Trusted Beneficiary no longer meets the requirements of the program or introduces unnecessary risk into the payments system.

ID# 0030632	Edition: Apr 2020 | Last Updated: Apr 2019

7.11.3.3   Delegated Authentication Program Transaction Processing – Europe Region

In the Europe Region: Transactions accepted by a Strong Customer Authentication Delegate in line with both 3-D Secure requirements and the Delegated Authentication Program must contain ECI value 7. An Acquirer will accept liability in line with Transactions that contain ECI value 7.

Visa Product and Service Rules

7 Transaction Processing

Visa Core Rules and Visa Product and Service Rules

ID# 0030620	Edition: Apr 2020 | Last Updated: Oct 2019

8   Processing Products

8.1   Use of Visa Systems

8.1.1   VisaNet Access Points

8.1.1.1   Deployment of Visa Systems at User Sites – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A participating Member, VisaNet Processor, or Visa Direct Connect Merchant that deploys a Visa system must provide, at no cost to Visa, all of the following:

- A location that meets Visa requirements for installing one or more VisaNet Access Points on the Member's, VisaNet Processor's, or Visa Direct Connect Merchant's premises

- A sufficient number of qualified personnel that the Member, VisaNet Processor, or Visa Direct Connect Merchant has trained to meet Visa specifications

- Upon Visa request, access to the premises of the Member, VisaNet Processor, or Merchant, and cooperation with Visa and its authorized agents or representatives for the installation, service, repair, or inspection of the VisaNet Access Points

- Computer time and a sufficient number of qualified personnel to ensure prompt and efficient installation and use of the VisaNet software supplied by Visa

- Any other support reasonably requested by Visa for the installation of Visa systems

A participating Member, VisaNet Processor, or Visa Direct Connect Merchant must do all of the following:

- Maintain VisaNet records, documents, and logs and provide them to Visa upon request

- Notify Visa promptly if a VisaNet Access Point for which it is responsible fails to operate properly

ID# 0027076	Edition: Apr 2020 | Last Updated: Oct 2019

8.1.1.2   Prohibition against VisaNet Access Point Modification

No party may make or attempt to make any repair, adjustment, alteration, or modification to a VisaNet Access Point, except as expressly authorized by Visa.

ID# 0027074	Edition: Apr 2020 | Last Updated: Oct 2014

8.1.1.3   VisaNet Access Point Security – Visa Direct Connect

A Visa Direct Connect Merchant must provide the same level of security for its VisaNet Access Points as it provides for its proprietary systems.

ID# 0027075   Edition: Apr 2020 | Last Updated: Oct 2019

8.1.2   Direct Connection to VisaNet

8.1.2.1   Visa Direct Connect Transaction Delivery

An Acquirer of a Visa Direct Connect Merchant must both:

- Be capable of receiving VisaNet reports or records as notification that both:
  - Clearing and Settlement occurred for Transactions submitted by the Visa Direct Connect Merchant
  - Payment is due to the Visa Direct Connect Merchant
- Accept responsibility for Transactions submitted by the Visa Direct Connect Merchant

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing.*

ID# 0027077   Edition: Apr 2020 | Last Updated: Apr 2018

8.1.3   System Changes

8.1.3.1   Visa Responsibilities Related to System Changes – Europe Region

In the Europe Region: Visa will provide to Members:

- 6 months' notice of changes that affect the systems and software of Members
- 2 Edit Package updates to be implemented in April and October of each year
- 3 weeks' notice for Visa Extended Access changes that do not affect Members

---

ID# 0029561   Edition: Apr 2020 | Last Updated: Oct 2016

8.2   Cardholder Loyalty Programs

8.2.1   Visa Loyalty Platform Services

8.2.1.1   Visa Loyalty Platform Services Issuer Participation Requirements

An Issuer that participates in the Visa Loyalty Platform Services must do all of the following:

- Obtain required consent from Cardholders and Merchants
- Within 10 calendar days of receiving the applicable Funds Disbursement from Visa (if applicable), credit to the participating Cardholder's account the amount of the discount received for qualifying purchases
- Not change the originating Merchant name and city information before posting this information to the Cardholder statement

ID# 0025865	Edition: Apr 2020 | Last Updated: Oct 2017

8.2.2   Card Linked Offers – Europe Region

8.2.2.1   Card Linked Offers Registration and Eligibility – Europe Region

In the Europe Region: An Issuer may, at its own option and where the service is available, register with Visa to join the Card Linked Offers Service. An Issuer that joins the Card Linked Offers Service must:

- Determine which of its Cardholders are eligible to join the service. Those Cardholders will register directly with Visa
- Provide Visa with the details of all eligible BINs that Issuer decides to include

An Issuer that participates in the Card Linked Offers Service must pay the associated fees to Visa as specified in the applicable fee schedule.

ID# 0030561	Edition: Apr 2020 | Last Updated: Apr 2018

8.2.2.2   Card Linked Offers Transaction Processing – Europe Region

In the Europe Region: An Issuer must process all payments associated with the Card Linked Offers Service as Original Credit Transactions to the Payment Credential of the Cardholder's registered Card.[1]

[1] An Original Credit Transaction associated with the Card Linked Offers Service will not carry an Interchange

Reimbursement Fee (IRF).

| ID# 0030562 | Edition: Apr 2020 \| Last Updated: Apr 2020 |

8.2.2.3   Card Linked Offers Transaction Data – Europe Region

In the Europe Region: An Issuer whose Cardholder has registered with Visa for the Card Linked Offers Service must provide Transaction data to Visa, including:

- All Transaction data linked to that Cardholder's Card for the 18 months before the date of registration
- On a daily basis, all Transaction data linked to that Cardholder's Card after the date of registration

Visa may, at the Issuer's option and on the Issuer's behalf, receive Transaction data from the Issuer's Visa Scheme Processor.

The Transaction data that Visa receives as part of the Card Linked Offers Service will be used in line with Visa's privacy policy, as provided to Cardholders before registering for the Card Linked Offers Service.

| ID# 0030563 | Edition: Apr 2020 \| Last Updated: Apr 2018 |

8.2.2.4   Card Linked Offers Marketing – Europe Region

In the Europe Region: An Issuer is responsible for marketing activities and communications associated with the Card Linked Offers Service provided to that Issuer's Cardholders, as specified in the *Visa Product Brand Standards*.

Visa reserves the right to review and amend an Issuer's communications and co-ordinate such communications with Merchants that provide offers, as agreed with the Issuer.

| ID# 0030564 | Edition: Apr 2020 \| Last Updated: Apr 2018 |

8.2.2.5   Card Linked Offers Use of Marks – Europe Region

In the Europe Region: To the extent that Visa has permission from a Merchant, Visa will provide a Member with a license to use that Merchant's branding. Such license must only be used:

- In association with the Card Linked Offers Service
- In accordance with that Merchant's brand guidelines, as communicated by Visa
- Subject to Visa's instruction, as determined from time to time

| ID# 0030565 | Edition: Apr 2020 \| Last Updated: Apr 2018 |

8.3 Visa Information Systems

8.3.1 Visa Online

8.3.1.1 Use of Visa Online

A Member, a VisaNet Processor, and any other authorized user that use Visa Online are subject to the Visa Online participation requirements.

A Member is responsible for a designated VisaNet Processor or other authorized user's use of the Visa Online materials, software, and information.

Visa Online and the information obtained through Visa Online are the property of Visa and are for the sole use of Members, VisaNet Processors, and other authorized users in support of Visa programs. A Member, VisaNet Processor or any other authorized user must not disclose any information from Visa Online unless permitted by the Visa Rules or otherwise authorized in writing by Visa.

ID# 0026950	Edition: Apr 2020 | Last Updated: Oct 2017

8.3.2 VisaVue Online

8.3.2.1 VisaVue Online Member Participation Requirements

To use VisaVue Online, a Member must sign a *VisaVue Member Participation Agreement*.

ID# 0026471	Edition: Apr 2020 | Last Updated: Oct 2017

8.4 Original Credit Transactions

8.4.1 Original Credit Transactions – Originating Requirements

8.4.1.1 Original Credit Transaction Limitations

An Original Credit Transaction must involve only a single sender and a single recipient.

ID# 0025765	Edition: Apr 2020 | Last Updated: Oct 2016

8.4.1.2   Original Credit Transactions – Treatment of Sender Data

An Originating Acquirer, either itself, or through its Merchants or service providers that originate an Original Credit Transaction, must:

- Validate sender data and comply with applicable anti-money laundering regulations and anti-terrorist financing standards, as specified in the *Visa Direct Original Credit Transaction (OCT) Global Implementation Guide*
- Provide proper disclosure to the sender regarding the collection of sender data

The Originating Acquirer must notify Visa before it or its Merchant or service provider start to process any Original Credit Transactions.

ID# 0005328	Edition: Apr 2020	Last Updated: Oct 2018

8.4.1.3   Original Credit Transaction Verification of Posting

To request confirmation or proof from a Recipient Issuer that funds have been posted to a recipient Cardholder's account, an Originating Acquirer must submit its inquiry through Visa Resolve Online.

The Recipient Issuer must respond to the Originating Acquirer's confirmation request through Visa Resolve Online within 5 calendar days from the date of inquiry.

ID# 0027329	Edition: Apr 2020	Last Updated: Oct 2018

8.4.1.4   Original Credit Transaction Reversals

An Originating Acquirer, a Merchant, or a service provider must not reverse an Original Credit Transaction initiated as an Online Financial Transaction.

A Reversal of an Original Credit Transaction must be processed within one business day of the Processing Date of the Original Credit Transaction and only for the following reasons:

- Incorrect Payment Credential
- Incorrect Transaction amount
- Duplicate processing
- Incorrect Transaction code

ID# 0026074	Edition: Apr 2020	Last Updated: Apr 2020

8.4.1.6   Conditions for Submission of an Original Credit Transaction Adjustment

An Originating Acquirer may submit a Transaction Adjustment if the Recipient Issuer fails to provide confirmation of posting of the Original Credit Transaction within 5 calendar days of the inquiry date.

The Original Credit Transaction Adjustment must be submitted within 30 calendar days of the Processing Date of the initial Original Credit Transaction.

ID# 0027330	Edition: Apr 2020 | Last Updated: Oct 2018

8.4.2   Original Credit Transactions – Recipient Issuer Requirements

8.4.2.1   Original Credit Transaction (OCT) Recipient Issuer Requirements

A Recipient Issuer must do all of the following:

- Post an Original Credit Transaction (OCT) to the Payment Credential within 2 business days[1] of receipt, or dispute the OCT to the Originating Acquirer
- If participating in Fast Funds, make funds available to the Cardholder within 30 minutes of approving an OCT
- For an OCT sent to a Cardholder's Credit Card account, post the funds as a payment
- For a Dispute processed for an OCT, only initiate a Dispute Reversal within one calendar day of the Dispute Processing Date
- Clearly describe the payment on the Cardholder statement and not label the payment as a refund
- Not apply additional funds transfer fees for consumer Cards

[1] In the Europe Region: For an Intraregional Transaction, on the same business day. The funds must be made available on the same business day.

ID# 0004064	Edition: Apr 2020 | Last Updated: Apr 2020

8.4.2.2   Original Credit Transactions – Conditions for Use of a Deposit-Only Account Number

A Recipient Issuer must:

- Notify Visa that a BIN or Account Range is designated for Deposit-Only Account Numbers
- Not use a Deposit-Only Account Number for any purpose other than Original Credit Transaction

processing

- List a compromised Deposit-Only Account Number on the Exception File

ID# 0006983		Edition: Apr 2020	Last Updated: Apr 2019

8.4.4 Original Credit Transactions – Fast Funds

8.4.4.1 Original Credit Transactions – Fast Funds Processing

A Recipient Issuer must process as Fast Funds an incoming Original Credit Transaction, if the following conditions are met:

Table 8-1: Fast Funds Processing Requirements

Region	Conditions
AP	The Recipient Issuer supports the receipt of Online Financial Transactions or Authorization Requests in the enhanced format.
CEMEA	
Europe	The Recipient Issuer supports the receipt of Online Financial Transactions or Authorization Requests in the enhanced format for a Reloadable Prepaid Card,[1] a Direct (Immediate) Debit Card, or a Deferred Debit Card.
Canada	The Original Credit Transaction is received for a Debit Card, a Reloadable Prepaid Card, or a Plus Program Card.
LAC	The Original Credit Transaction is received for a Debit Card or a Prepaid Card.
US	The Recipient Issuer supports the receipt of Online Financial Transactions or Authorization Requests in the enhanced format. **Effective through 16 April 2021** This does not apply to an incoming Original Credit Transaction to a Credit Card.
[1] Applies only to Prepaid Accounts where full Cardholder due diligence, such as KYC, has been completed to the Issuer's satisfaction	

ID# 0027273		Edition: Apr 2020	Last Updated: Apr 2020

8.4.4.2   Online Original Credit Transaction Origination

An Originating Member must use an enhanced format 0200 message to initiate an online Original Credit Transaction.

| ID# 0027274 | Edition: Apr 2020 | Last Updated: Apr 2017 |

8.5   Mobile Push Payment Transactions

8.5.1   Mobile Push Payment Transactions – Issuer Requirements

8.5.1.1   Payment Credential Assignment for Mobile Push Payment Program

An Issuer that enables Mobile Push Payment Transactions must ensure that a Mobile Push Payment Transaction uses either:

- The Account Number of a physical Card issued to the Cardholder
- The Payment Credential issued from a Visa Classic BIN or Account Range if a physical Card has not been issued to the account holder

| ID# 0030581 | Edition: Apr 2020 | Last Updated: Apr 2020 |

8.5.1.2   Electronic Transaction Receipt Requirements for Mobile Push Payment Transactions

For a Mobile Push Payment Transaction, an Issuer must provide a completed electronic Transaction Receipt to the Cardholder that includes all of the following elements:

Table 8-2: Required Electronic Transaction Receipt Content for Mobile Push Payment Transactions

Required Element	Additional Requirements
Payment Credential	The Payment Credential, except for the final 4 digits, must be disguised or suppressed on the Cardholder's copy of an electronic Transaction Receipt.
Authorization Code	No additional requirements apply
Card network name	Must contain "Visa"
Merchant location	The city and state/province of the Merchant Outlet
Merchant name	The name the Merchant uses to identify itself to its customers

Table 8-2: Required Electronic Transaction Receipt Content for Mobile Push Payment Transactions (continued)

Required Element	Additional Requirements
Transaction amount	Total currency amount of all goods and services sold to the Cardholder at the same time, including applicable taxes and fees and any adjustments or credits
Transaction Date	No additional requirements apply
Transaction type	One of the following: • Cash-In • Cash-Out • Refund • Purchase

In addition, the Issuer must do both of the following:

• Provide clear instructions to the Cardholder for accessing the electronic Transaction Receipt

• Make the receipt available to the Cardholder for at least 120 calendar days after the Processing Date

ID# 0030584   **Edition: Apr 2020 | Last Updated: Apr 2020**

8.6   Visa Processing Services

8.6.1   Visa Account Updater

8.6.1.1   Issuer Use of Visa Account Updater

An Issuer enrolled in Visa Account Updater (VAU) must do all of the following:

• Agree and acknowledge that Visa may use, store, update, or disclose the Issuer's data, in accordance with applicable laws or regulations, regarding the personal data that Visa or its subcontractor stores and processes on behalf of Members participating in VAU to:

   – Facilitate the use of VAU by an Acquirer or a Merchant

   – Support other Visa services

• Comply with all data protection requirements

Visa Core Rules and Visa Product and Service Rules

- Submit updates for Cards under its enrolled BINs whenever reissuance or a change in account status occurs, as specified in *Table 8-3, VAU Issuer Update Requirements,* for the following:

  – AP Region

  – Canada Region

  – **Effective 17 October 2020** CEMEA Region

  – Europe Region (except Greece, Italy, Republic of Ireland, United Kingdom)

  – LAC Region

  – US Region

Table 8-3: VAU Issuer Update Requirements

VAU Update Type	Requirements

Account Number and Expiration Date Change	• Permitted only if both:
	   – The Account Number has been activated.
	   – An Authorization Request using the updated data can be approved.
	 • Must be submitted within 2 business days of Account Number activation

"Closed Account" Advice	Permitted only if the closure is permanent (the account can never be reopened using that Account Number)
"Contact Cardholder" Advice	Permitted only if either: • The Cardholder requests that specific new information not be provided. • The Issuer cannot or will not provide specific information for risk reasons.
"Opt-Out" Advice	Permitted only if the Cardholder requests that specific new information not be provided

If inaccurate information is supplied to VAU, the Issuer must do all of the following:

- Promptly investigate any claims of inaccuracies

- Immediately notify Visa of any inaccuracies

- Remove inaccurate information from VAU within 2 business days of notification and provide corrected information within 5 business days of notification

An Issuer must enroll its BINs in VAU, as follows:

Table 8-4: VAU Enrollment Requirements – Canada Region, CEMEA Region, Europe Region, US Region

Region	Country	BIN Enrollment Requirements
Canada	N/A	All BINs, except: • Visa Commercial Card BINs • Prepaid Card BINs • Licensed BINs for ATM-only Cards
Effective 17 October 2020 CEMEA	All	All BINs: • Except Non-Reloadable Prepaid Card BINs • Unless the Issuer supports life cycle management associated with Tokens and their underlying primary Account Numbers, including, but not limited to, Account Number updates and expiration date updates
Europe	Greece Italy Republic of Ireland United Kingdom **Effective through 17 April 2020** Czech Republic Finland Poland Slovakia Spain Sweden **Effective 18 April 2020** All, except Hungary, Switzerland, and Turkey	All BINs, except Prepaid Card BINs
	Switzerland	All BINs, except: • Prepaid Card BINs • BINs shared by more than one Issuer
US	N/A	All BINs, except:

Table 8-4: VAU Enrollment Requirements – Canada Region, CEMEA Region, Europe Region, US Region (continued)

Region	Country	BIN Enrollment Requirements
		• Visa Commercial Card BINs • Prepaid Card BINs • BINs licensed for use in US Territories

ID# 0029869   Edition: Apr 2020 | Last Updated: Apr 2020

8.6.2 Visa Payment Controls

8.6.2.1 Visa Payment Controls – Issuer Participation Requirements

An Issuer that participates in Visa Payment Controls must do all of the following:

- Submit to Visa a completed *Visa Payment Controls Client Information Questionnaire* before offering the service
- Offer the service for the following products:
  - Visa Consumer Card, Visa Commercial Card, or Prepaid Card
  - In the US Region: A Visa Consumer Credit Card or Visa Commercial Credit Card
- Provide Visa with Payment Credentials that are enrolled in the service

ID# 0027238   Edition: Apr 2020 | Last Updated: Apr 2020

8.6.3 Straight Through Processing

8.6.3.2 Straight Through Processing – Acquirer Participation Requirements

To participate in Straight Through Processing an Acquirer must register with Visa and sign a *Straight Through Processing Participation Agreement*.

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing*.

ID# 0030129   Edition: Apr 2020 | Last Updated: Apr 2018

8.7 Visa Software

8.7.1 Software License

8.7.1.2 Indemnification Related to Licensed Software

A Member agrees to Indemnify Visa for and against Claims or Liabilities arising out of or in connection with a software license, the software, or the use thereof.

ID# 0029984	Edition: Apr 2020	Last Updated: Apr 2018

8.7.1.6 Prohibition Against Issuer Use of Open Source Software

A Member must not incorporate, link, distribute or use any third party or open source software (including without limitation, any open source license listed on *http://www.opensource.org/licenses/alphabetical*) (each, an "open source license") or code in conjunction with any Visa products, software, services, application programming or other interfaces, or other Visa technologies, in a way that may result in any of the following:

- Create obligations with respect to, or require disclosure of, any Visa technology, including without limitation the distribution or disclosure of any application programming interfaces or source code relating to such interfaces

- Grant to any third party any rights to or immunities under any Visa (or any Visa affiliates) intellectual property rights or proprietary rights

- Cause any Visa technology to become subject to the terms of any open source license

ID# 0029518	Edition: Apr 2020	Last Updated: Apr 2017

9   Interchange

The content of Chapter 9 may be found in *Section 1.9, Interchange,* and the applicable Interchange Reimbursement Fee (IRF) documentation.

ID# 0030089	Edition: Apr 2020 | Last Updated: Oct 2017

10   Risk

10.1   Corporate Risk Reduction

10.1.1   Acquirer Risk Responsibilities

10.1.1.2   Acquirer Risk Policies – US Region

In the US Region: An Acquirer must implement, and its board of directors must approve, all of the following:

- An underwriting, monitoring, and control policy for all of the following:
  - Its Merchants
  - Its VisaNet Processors
  - Its Third Party Agents
- A policy and procedures for reviewing solicitation materials used by its Agent

The Acquirer must provide policies to Visa upon request.

ID# 0007132	Edition: Apr 2020 | Last Updated: Oct 2014

10.1.1.3   Acquirer Responsibility for Agents and Merchants – US Region

In the US Region: An Acquirer must:

- Provide its Agents with training and education, as specified by Visa, and ensure that Agents are in compliance with the Acquirer's corporate policies
- Hold and control reserves that are accumulated and derived from Merchant settlement funds or used to guarantee a Merchant's payment system obligations to the Member

ID# 0002110	Edition: Apr 2020 | Last Updated: Oct 2014

10.1.2   Electronic Commerce Merchant Requirements

10.1.2.1   Electronic Commerce Transaction Type Prohibition

A Merchant, Payment Facilitator, Sponsored Merchant, or entity classified as high-brand risk, as specified in *Section 10.4.6.1, High-Brand Risk Merchants,* that displays a Visa-Owned Mark on its website and/or application must not accept Cards for either:

- The purchase or trade of photographs, video imagery, computer-generated images, cartoons, simulation, or any other media or activities including, but not limited to, activities listed in *Section 1.3.3.4, Brand Protection and Use of the Visa-Owned Marks*
- The purchase of products that claim or imply a similar efficacy as prescription drugs, controlled substances, or recreational/street drugs, irrespective of claims of legality

Violation of this requirement may result in the termination of the Merchant, Payment Facilitator, Sponsored Merchant, High-Brand Risk Merchant, High-Risk Internet Payment Facilitator, or High-Brand Risk Sponsored Merchant.

ID# 0005067	Edition: Apr 2020 | Last Updated: Oct 2019

10.1.2.2 High-Risk Merchants Offering Online Storage or File-Sharing Services – Europe Region

In the Europe Region: A Merchant or Sponsored Merchant will be classified as high-risk if any of the following apply:

- Users of the Merchant or Sponsored Merchant's service are rewarded for uploading, downloading, or sharing content
- The Merchant or Sponsored Merchant promotes online content by distributing URL codes or forum codes to individuals or third parties
- There is a link-checker on the Merchant or Sponsored Merchant's website and/or application, allowing individuals to check whether a link has been disabled in order to re-upload content that has previously been removed

Visa reserves the right to determine whether a Merchant or Sponsored Merchant that offers online storage and file sharing services is classified as high-risk.

An Acquirer of a Merchant or Sponsored Merchant that offers online storage and file sharing services and that is classified as high-risk must both:

- Ensure that the Merchant or Sponsored Merchant cancels the contract of individuals that have uploaded illegal content, and ensure that those individuals cannot upload any content in the future
- Ensure that the Merchant or Sponsored Merchant gathers enough information about individuals that use their service to identify them to law enforcement authorities if they upload illegal content

ID# 0029662	Edition: Apr 2020 | Last Updated: Apr 2018

10.1.2.3   Online Storage and File-Sharing Merchants – Europe Region

In the Europe Region: An Acquirer of a Merchant or Sponsored Merchant that offers the purchase or use of online storage and file-sharing services must ensure that the Merchant or Sponsored Merchant both:

- Implements a process for reviewing, removing, and reporting illegal or prohibited content and prevents individuals who have uploaded illegal or prohibited content from uploading any content in the future
- Reports all illegal content to the relevant authorities based on the local laws governing the country in which any of the following apply:
  - The Merchant or Sponsored Merchant has its Merchant Outlet.
  - The illegal content is stored.
  - The illegal content is uploaded and/or downloaded.

ID# 0029799	Edition: Apr 2020 | Last Updated: Oct 2016

10.1.3   Anti-Money Laundering

10.1.3.1   Anti-Money Laundering Program Overview

Visa maintains an anti-money laundering program reasonably designed within the context of laws and regulations applicable to Visa to prevent the Visa system from being used to facilitate money laundering or the financing of terrorist activities.

ID# 0003969	Edition: Apr 2020 | Last Updated: Oct 2014

10.1.3.2   Anti-Money Laundering/Anti-Terrorist-Financing Program – ATM Acquirers

An ATM Acquirer must ensure that it has in place policies, controls, and procedures to minimize the risk of its ATMs being used to facilitate money laundering or terrorist financing, and submit any required currency transaction reports or suspicious activity reports to its regulator.

If the ATM Acquirer uses a Third Party Agent to load funds to its ATMs, the ATM Acquirer must require and compel such Third Party Agent to comply with all applicable laws and regulations, including without limitation, laws regarding anti-money laundering and anti-terrorist financing. The ATM Acquirer must maintain and enforce a program that, at minimum, includes conducting appropriate due diligence on each Third Party Agent, requiring adequate record keeping and validation of source of funds, and conducting regular, ongoing independent audits to confirm the Third Party Agent's compliance. The ATM Acquirer will be responsible to Visa for any acts or omissions of the ATM Acquirer's Third Party Agents.

ID# 0028291	Edition: Apr 2020 | Last Updated: Oct 2014

10.1.4   Blocking of BINs and Acquiring Identifiers

10.1.4.1   BIN and Acquiring Identifier Blocking by Visa – Europe Region

In the Europe Region: Visa may, as it sees fit at any time and without warning, require a Visa Scheme Processor to block the function of all or any part of its system in relation to any BIN or Acquiring Identifier assigned to a Member (a "blocked BIN or Acquiring Identifier") so that, during the period of the block, one or more of the following:

- No Authorization may be given using the blocked BIN or Acquiring Identifier.
- No Clearing Record may be created in respect of the blocked BIN or Acquiring Identifier.
- No Settlement may be effected of amounts owed to the blocked BIN or Acquiring Identifier.

(any such outcome being a "BIN or Acquiring Identifier block") subject only to such exceptions as Visa may see fit to make from time to time.

Visa will exercise its discretions under this paragraph with a view to all of the following (each being "BIN or Acquiring Identifier blocking objective"):

- Ensuring the stability of the Visa system
- Protecting Visa and its Members from incurring Liability (including, without limitation, in respect of Settlement Loss)
- Avoiding or mitigating any act or omission that Visa considers might be illegal, inconsistent with applicable regulatory standards, or materially damaging to the Visa brand

Visa may declare any BIN or Acquiring Identifier block to be temporary, indefinite, or permanent. If no such declaration is made, a BIN or Acquiring Identifier block will be treated as indefinite. Visa will take such steps as it considers appropriate to terminate the membership of any entity whose assigned BIN or Acquiring Identifier is subject to a permanent BIN or Acquiring Identifier block. A temporary or indefinite BIN or Acquiring Identifier block will end either:

- If Visa both:
    - Determines that continuing the BIN or Acquiring Identifier block is of no further help to achieving the BIN or Acquiring Identifier blocking objectives
    - Does not intend to terminate the membership of any entity to whom the blocked BIN or Acquiring Identifier is assigned
- In the case of a temporary BIN or Acquiring Identifier block only, if earlier, at the time and subject to such conditions that Visa may specify

Visa may at any time and without warning cancel a BIN or Acquiring Identifier block and/or change the status and scope of application of any BIN or Acquiring Identifier block. Visa may at any time and without warning extend or modify the conditions of any temporary BIN or Acquiring Identifier block.

Visa's right to effect a BIN or Acquiring Identifier block is in addition, and without prejudice, to any other rights or remedies of Visa under the Member Agreements and the Visa Rules.

The exclusions and limitations of Visa's liability specified in the Visa Rules will apply to any Claims or Liabilities arising out of or in connection with a BIN or Acquiring Identifier block.

ID# 0029565	Edition: Apr 2020 | Last Updated: Oct 2019

10.1.5   Crisis Management and Business Continuity – Europe Region

10.1.5.1   Crisis Management and Business Continuity Requirements – Europe Region

In the Europe Region: A Member must do all of the following:

- Maintain an effective crisis management and business continuity program and ensure that the program includes a plan for ensuring recovery or continuity of the Member's critical business activities, services, and technology solutions
- Ensure that, if any critical activity or service is outsourced to a third party, the third party maintains a similar crisis management and business continuity program
- Upon Visa request, provide evidence of the existence and effectiveness of a Member's or third party's crisis management and business continuity program

ID# 0029562	Edition: Apr 2020 | Last Updated: Oct 2016

10.2   Agents and Processors

10.2.1   Member Requirements Related to VisaNet Processors and Visa Scheme Processors

10.2.1.1   VisaNet Processor Contracts

A Member must execute a written contract with each VisaNet Processor or Visa Scheme Processor. The contract must comply with all of the following:

- Include minimum standards established by Visa, including, but not limited to:
  - Policies
  - Procedures
  - Service levels
  - Performance standards
- Include language that:
  - Permits Visa to conduct financial and procedural audits and general reviews at any time
  - Requires the VisaNet Processor or Visa Scheme Processor to make Cardholder and Merchant information available to Visa and regulatory agencies
  - Contains a notice of termination clause
- Require that the VisaNet Processor or Visa Scheme Processor comply with:
  - The Visa Rules
  - Applicable laws or regulations
- Be executed by a senior officer of the Member
- Require the VisaNet Processor or Visa Scheme Processor to comply with the _Payment Card Industry Data Security Standard (PCI DSS)_
- Require that the VisaNet Processor or Visa Scheme Processor be properly registered with Visa

ID# 0025879	Edition: Apr 2020 | Last Updated: Oct 2014

10.2.1.2   VisaNet Processor and Visa Scheme Processor Systems Agreement

Visa may require a Member's VisaNet Processor or Visa Scheme Processor to enter into an agreement directly with Visa before the delivery of any of the following:[1]

- BASE II software
- Visa Extended Access server or Visa Extended Access Proxy server
- Other systems determined by Visa

The agreement may specify terms and conditions for the use of software or equipment that Visa determines necessary to protect its proprietary rights. This provision does not require Visa to agree to this type of arrangement, nor does it give any VisaNet Processor or Visa Scheme Processor the right to use VisaNet.

[1] In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in _Section 1.1.1.2_

Applicability of Processing Rules – Europe Region, it must refer to *Visa Europe Operating Regulations – Processing.*

ID# 0025882	Edition: Apr 2020 | Last Updated: Oct 2019

10.2.1.3   VisaNet Processor, Payment Facilitator, Staged Digital Wallet Operator, and Marketplace Agreement – LAC Region (Brazil)

In the LAC Region (Brazil): A VisaNet Processor, a Marketplace, a Payment Facilitator, and a Staged Digital Wallet Operator must enter into an agreement directly with Visa before the delivery of any services to Members.

This provision does not require Visa to agree to this type of arrangement, nor does it give any VisaNet Processor the right to use VisaNet.

ID# 0029221	Edition: Apr 2020 | Last Updated: Apr 2018

10.2.1.4   VisaNet Processor Requirements Related to Third Parties

A contract between a Member and its VisaNet Processor or Visa Scheme Processor must require the VisaNet Processor or Visa Scheme Processor to:

- Ensure that any third party that uses the Member's BIN or Acquiring Identifier is properly registered with Visa by that Member
- Notify BIN Licensees or Acquiring Identifier Licensees in writing and receive written approval before allowing a Third Party Agent to use the Member's BIN or Acquiring Identifier, or granting access to Cardholder information
- Report at least quarterly to the Member and Visa any third party that uses its BIN or Acquiring Identifier

ID# 0025881	Edition: Apr 2020 | Last Updated: Oct 2019

10.2.1.5   General Member Responsibilities for VisaNet Processors and Visa Scheme Processors

A Member that has a contract with a VisaNet Processor or a Visa Scheme Processor must:

- Provide Transaction-related processing instructions directly to its VisaNet Processor or Visa Scheme Processor
- Distribute written policies and procedures to its VisaNet Processors or Visa Scheme Processors[1]

- Establish a risk management program to control risks related to the use of VisaNet Processors or Visa Scheme Processors, such as:
  - Loss of operational control
  - Service provider failure
  - Confidentiality and physical and logical security of Cardholder and Visa Transaction Information
- Verify that the principals and senior management of the VisaNet Processor or Visa Scheme Processor have the requisite knowledge and experience to successfully perform the contracted services[2]
- Conduct from time to time an on-site inspection of the business premises[2] to:
  - Verify inventory
  - Inspect operational controls
  - Monitor security standards regarding unauthorized disclosure of or access to Visa data and other payment systems
- Immediately notify Visa of any change in the VisaNet Processor or Visa Scheme Processor relationship, including termination, change of ownership or business function, or processor[3]
- Ensure that any changes to BIN or Acquiring Identifier relationships comply with the applicable licensing requirements
- In the Europe Region: Provide relevant rules to its Visa Scheme Processor
- In the Europe Region: After discontinuing a Visa Scheme Processor relationship, maintain a file on the processor that includes records of all applicable due diligence and retain this file, with the reason for discontinuance, for a minimum of 2 years

In the Europe Region: A Visa Scheme Processor must not imply that its registration with Visa is an endorsement of its services by Visa.

[1]   In the Europe Region: Visa may permanently prohibit a Visa Scheme Processor or one of its principals, or any of its agents, from accessing VisaNet for good cause.

[2]   Except when a VisaNet Processor or Visa Scheme Processor is a Member or special Licensee.

[3]   In the Europe Region: Within 5 business days.

ID# 0025880   **Edition: Apr 2020 | Last Updated: Oct 2019**

10.2.1.6   Procedures for Use of an Airline Authorizing Processor

Before implementing a direct connection to VisaNet, a Member must ensure that its Airline Authorizing Processor has either:

- Completed and submitted to Visa a *VisaNet Letter of Agreement*

- Signed a separate agreement with Visa

If a Member that acquires Airline Transactions is using an approved Airline Authorizing Processor, the Member is not required to submit a *VisaNet Letter of Agreement* or *VisaNet Processor and Third Party Registration and Designation*.

ID# 0001021	Edition: Apr 2020 | Last Updated: Oct 2014

10.2.1.7 Requirements for VisaNet Processor and Visa Scheme Processor Marketing Materials

A Member must require that its VisaNet Processor or Visa Scheme Processor:

- Uses only marketing materials approved by the Member

- Ensures that all marketing materials displaying the Visa-Owned Marks also include the Member name,[1] which must be more prominent and in a larger font than that of the VisaNet Processor or Visa Scheme Processor

- Is prominently identified on the marketing materials as an agent or representative of the Member, unless the Member has provided its approval to exclude its name from such marketing materials

- For Prepaid Card distribution, ensures that any website and/or application displaying the Visa-Owned Marks or offering Visa Card services clearly and conspicuously includes the Member name, which must be located close to the Visa-Owned Marks

[1] In the Canada Region: With Member approval and provided that the Acquirer Processor has entered into the form of Trademark License Agreement for Acquirer Processors as prescribed by Visa, a Member's Acquirer Processor may display certain Visa-Owned Marks on its marketing materials without the Member's name or logo in accordance with the terms of the Trademark License Agreement for Acquirer Processors.

ID# 0025885	Edition: Apr 2020 | Last Updated: Apr 2020

10.2.1.8 Non-Member VisaNet Processor or Clearing Member Reporting

A Member that uses a non-Member VisaNet Processor or Clearing Member to process Transaction-related data must submit, upon request, an annual report to Visa that includes at least all of the following:

- Identification of the services provided by the non-Member VisaNet Processor or Clearing Member

Visa Core Rules and Visa Product and Service Rules

- Products and programs supported

- BINs or Acquiring Identifiers under which the Member's activity is processed

ID# 0025874	Edition: Apr 2020 | Last Updated: Oct 2019

10.2.1.9   VisaNet Processor Independent Audit – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Upon designation of a VisaNet Processor, a sponsoring Member must obtain and review an independent audit of the internal controls that support the VisaNet Processor's VisaNet interface.[1] The audit must be conducted annually and use standard audit practices of the International Audit Standards or other regionally acceptable standards agreed by Visa.

[1] This does not apply if the VisaNet Processor is a Member or special Licensee.

ID# 0025878	Edition: Apr 2020 | Last Updated: Oct 2016

10.2.1.10   VisaNet Processor Acting as Clearing Processor

A Member must ensure that its Clearing Processor:

- Provides access to Cardholder, Merchant, Marketplace, Sponsored Merchant, Payment Facilitator, Digital Wallet Operator, and Member data

- Withholds or redirects Settlement funds, as required by Visa

ID# 0025883	Edition: Apr 2020 | Last Updated: Apr 2018

10.2.1.11   Visa Collection of Funds from a Member or VisaNet Processor – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: In collecting funds owed by a Member or VisaNet Processor, Visa may take, but is not limited to, the following actions:

- Take and liquidate collateral posted by a Member or VisaNet Processor, as specified in the agreement for the posting

- After providing at least one business day's notice before the collection, either:

  – Debit the Member's or VisaNet Processor's Clearing account through VisaNet

  – Withhold amounts from payments that Visa owes to the VisaNet Processor

In the US Region: A Member or VisaNet Processor must remit the total amount owed, as specified in the *Visa International Certificate of Incorporation and By-Laws*.

In the US Region: If a Member or VisaNet Processor does not remit the amount owed, the Member is responsible for Visa expenses incurred in collecting the funds, including, but not limited to, costs and expenses of legal action.

In the US Region: A Member from whom Visa collects amounts due must continue to honor its obligations to Merchants and Sponsored Merchants.

In the US Region: A VisaNet Processor must not charge a Member's Clearing account unless either:

- Visa has directed the VisaNet Processor to do so
- The Member whose account is to be charged has provided written consent for the charge and the consent does not prevent the Member from complying with the Visa Rules

In the US Region: Visa is not required to exhaust its remedies in collecting from one Member or VisaNet Processor before collecting from another Member.

ID# 0025889	Edition: Apr 2020	Last Updated: Oct 2016

10.2.1.12   Member or VisaNet Processor Dispute of Amount Collected by Visa – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: If a Member or VisaNet Processor wishes to dispute an amount collected by Visa, it must both:

- Provide written notice to Visa within 60 calendar days of the collection date, if it wishes to dispute its liability for or the amount of the collection
- Not withhold payment because the Member or VisaNet Processor disputes its liability for the payment

Visa is both:

- Liable only for the amount improperly collected plus interest at the prime rate in effect at the Settlement Bank used by Visa
- Not liable for collections made in error, except for intentional misconduct

ID# 0025891	Edition: Apr 2020	Last Updated: Oct 2016

10.2.2   Member Requirements Related to Third Party Agents

10.2.2.1   Member Risk Management and Approval for Third Party Agents

Before contracting with a Third Party Agent, a senior officer of a Member must review all documentation. The Member must do all of the following:

- Determine that the entity is financially responsible and adheres to sound business practices

- Comply with the Third Party Agent Registration Program

- Conduct a background investigation to verify the responsibility (including, where appropriate, financial responsibility) of the principals and ensure that no significant derogatory information exists. If applicable laws or regulations prohibit checks (including financial reviews) on individuals, the Member must note this when registering the Third Party Agent and note what other due diligence procedures were undertaken to ensure that due diligence was completed.

- Review the Program Request Management application or the appropriate regional form each time it signs a Third Party Agent

Approval of a Third Party Agent must not be based solely on any purported limitation of the Member's financial liability in any agreement with the Third Party Agent.

Registration of a Third Party Agent does not represent confirmation by Visa of the Third Party Agent's compliance with any specific requirement.

ID# 0025906   **Edition: Apr 2020 | Last Updated: Oct 2016**

10.2.2.2   Third Party Agent Contract Requirements

A Member must execute a written contract with each Third Party Agent that performs Cardholder or Merchant solicitation or stores, processes, or transmits Cardholder or Transaction data on behalf of the Member. The contract, to the extent permitted by applicable laws or regulations, must comply with all of the following:

- Include minimum standards established by Visa, including, but not limited to:
  - Policies
  - Procedures
  - Service levels
  - Performance standards

- Include language that:
  - Permits Visa to conduct financial and procedural audits and general reviews at any time
  - Requires the Third Party Agent to make Cardholder and Merchant information available to Visa and regulatory agencies
  - Contains a notice of termination clause
  - Permits Visa to determine the necessity of, and impose risk conditions on, the Third Party Agent
- Require that the Third Party Agent comply with:
  - The Visa Rules
  - Applicable laws or regulations
- Be executed by a senior officer of the Member
- Contain at least the substance of the provisions specified in *Section 10.2.2, Member Requirements Related to Third Party Agents*
- Require that the Third Party Agent comply with the *Payment Card Industry Data Security Standard (PCI DSS)*
- Include a provision allowing the Member or its Merchant to terminate the contract if the Third Party Agent participates in any of the activities described in *Section 10.2.2.11, Prohibition of Third Party Agents from Providing Services,* or the Member or its Merchant becomes insolvent

ID# 0025902	Edition: Apr 2020	Last Updated: Oct 2014

10.2.2.3   Third Party Agent On-Site Inspection

Before registering a Third Party Agent, a Member must perform an on-site inspection of the Third Party Agent's business location as part of the due diligence requirement to:

- Verify inventory, if applicable
- Review solicitation or sales materials
- Inspect operational controls
- Monitor security standards regarding unauthorized disclosure of, or access to, Visa Transaction Information and other payment systems' transaction information

Visa may conduct an on-site inspection of any Third Party Agent to validate its compliance with the applicable security requirements.

ID# 0025907	Edition: Apr 2020	Last Updated: Oct 2014

Visa Product and Service Rules

10 Risk

Visa Core Rules and Visa Product and Service Rules

10.2.2.4   Member and Third Party Agent Compliance with Due Diligence Standards

Before registering a Third Party Agent, a Member must complete and validate compliance with the applicable regional due diligence standards that are through the Program Request Management application or from Visa. Upon Visa request, a Member may be required to provide documentation to confirm compliance with regional due diligence standards.

A Member with a registered Third Party Agent must perform an annual review of the Third Party Agent to confirm ongoing compliance with applicable regional due diligence standards.

ID# 0025895	Edition: Apr 2020 | Last Updated: Oct 2016

10.2.2.5   Third Party Agent Change Notification

A Member must use the Program Request Management application or the appropriate form to notify Visa of any change in a Third Party Agent's principals or business relationship (including change of ownership or termination of contract). The Member must submit the notice to Visa within 5 business days of the change or knowledge of the change.

The Member must forward to Visa requests for correction.

ID# 0025899	Edition: Apr 2020 | Last Updated: Oct 2016

10.2.2.6   Member Requirements for Third Party Agents

A Member that uses a Third Party Agent must do all of the following:

- Identify the Third Party Agent to Visa using the Program Request Management application and designate the activities that it is authorized to perform on the Member's, or the Member's Merchant's, behalf
- Control the approval and review of Merchants, approval of Cardholder applications, and establishment of Merchant fees for Transactions
- Guarantee that it and the Third Party Agent will comply with Third Party Agent requirements and *Section 10.3, Account and Transaction Information Security*
- Ensure that the Third Party Agent has access to and uses the information contained in the Client Service Provider Directory, if the Member uses the Third Party Agent for processing any of the following:
  - Disputes
  - Arbitration cases
  - Compliance cases

- – Authorizations
- – Fraud reporting cases
- – Settlement

- Advise the Third Party Agent that:
  - – It must not represent registration in the Third Party Registration Program as Visa endorsement of its services
  - – Registration of a Third Party Agent is specific to each Member, and a separate Third Party Agent registration is required for each Member business relationship
- Accept responsibility for any and all losses caused by its Third Party Agent[1]
- After discontinuing a Third Party Agent relationship, maintain a file on the Third Party Agent that includes records of all applicable due diligence and retain this file, with the reason for discontinuance, for a minimum of 2 years
- Upon Visa request submit a detailed quarterly report, signed by an authorized officer, of the activities and services of each Third Party Agent doing business on its behalf. Visa may assess a non-compliance assessment if the Member fails to provide this information within 30 calendar days from the end of each quarter.

[1] In the Europe Region: A Member must include this provision in its agreement with the Third Party Agent.

ID# 0025909	Edition: Apr 2020 | Last Updated: Oct 2019

10.2.2.7   Member Responsibilities for Card Activities

A Member is responsible for all Card activities associated with Visa products and services, whether performed directly or indirectly by the Member or a Third Party Agent. The Member must, at a minimum, guarantee that:

- Its Merchants are paid for proper acceptance of a Card
- Payments received from Cardholders are applied for the purpose for which they were remitted

These obligations must not be waived, abrogated, or superseded in any manner.

ID# 0025910	Edition: Apr 2020 | Last Updated: Oct 2014

10.2.2.8   Third Party Agent Responsibility to Provide Cardholder or Merchant Information

If a Member, Visa or its designees, or any regulatory agency requests Cardholder or Merchant information of any type, a Third Party Agent must provide the information in writing no later than 7

business days from receipt of a request. If applicable laws or regulations prohibit the provision of the information, the Third Party Agent must note the exception when the original request is submitted.

| ID# 0025912 | Edition: Apr 2020 | Last Updated: Oct 2014 |

10.2.2.9   Requirements for Third Party Agent Solicitation and Marketing Materials

A Member must approve a Third Party Agent's use of any solicitation materials, such as advertisements, stationery, business cards, sales brochures, and website and/or application promotional content.

The Member must ensure all of the following if its Third Party Agent uses solicitation and marketing materials displaying the Visa-Owned Marks:

- The Member's name and headquarters city are prominently identified adjacent to the Visa-Owned Marks.

- Any subsequent Cardholder or Merchant Agreement is between the Member and the individual Cardholder or Merchant.

- On Cardholder solicitation materials, the Member, not the Third Party Agent, is noted as the Issuer of the Card.

- The material does not identify the Third Party Agent, unless the Third Party Agent is prominently identified as a representative of the Member.

- The Third Party Agent presents itself to all current and prospective Cardholders and Merchants under the Trade Name or "doing business as" (DBA) name registered with the Member.

- The Third Party Agent does not use a Visa-Owned Mark on marketing materials, such as business cards and letterhead on stationery.

| ID# 0025914 | Edition: Apr 2020 | Last Updated: Apr 2018 |

10.2.2.10   Disclosure of Account or Visa Transaction Information

A Member must ensure that a Third Party Agent with access to account or Visa Transaction Information complies with Visa Transaction Information security requirements, as specified in *Section 10.3, Account and Transaction Information Security*

In the event of the failure, including bankruptcy, insolvency, or other suspension of business operations of one of a Member's Third Party Agents, the Member must ensure that the Third Party Agent does not sell, transfer, or disclose any materials that contain Account Numbers, personal information, or other Visa Transaction Information to any other entity. The Member must ensure that its Third Party Agent either:

- Returns this information to the Member
- Provides to the Member acceptable proof of secure destruction of this information

ID# 0025917	Edition: Apr 2020 | Last Updated: Oct 2016

10.2.2.11   Prohibition of Third Party Agents from Providing Services

Visa may permanently prohibit a Third Party Agent and its principals from providing services with respect to Visa products for good cause, such as:

- Fraudulent activity
- Activity that causes the Member to repeatedly violate the Visa Rules
- Operating in an unsound, unsafe manner
- Any other activities that may result in undue economic hardship or damage to the goodwill of the Visa system, if the Third Party Agent fails to take corrective action

ID# 0025918	Edition: Apr 2020 | Last Updated: Oct 2014

10.2.2.12   Third Party Agent Operational Review – US Region

In the US Region: An Acquirer that does not meet the capital requirements specified in *Section 5.3.1.3, Acquirer Requirements for Contracting with Payment Facilitators,* must undergo a Global Acquirer Risk Standards operational review before approval of its first Third Party Agent registration for soliciting Merchants. The cost of the operational review is the responsibility of the Acquirer.

ID# 0025897	Edition: Apr 2020 | Last Updated: Oct 2016

10.2.2.13   Competitors as Agents – US Region

In the US Region: A Member must not appoint or permit as its Agent for Cardholder or Merchant solicitation any organization, or its respective subsidiaries or affiliates, that Visa deems to be a competitor.

ID# 0001166	Edition: Apr 2020 | Last Updated: Apr 2020

10.2.2.14   Agent Prohibitions Related to Visa-Owned Marks – US Region

In the US Region: An Agent of a Member must not:

Visa Core Rules and Visa Product and Service Rules

- Permit the use of any Visa-Owned Mark by any of its own agents
- Use any Visa-Owned Mark on any marketing material, including business cards and letterhead on stationery

ID# 0001168	Edition: Apr 2020 | Last Updated: Oct 2014

10.2.3   Member Requirements Related to Third Parties – Europe Region

10.2.3.1   Third Party Contract Requirements – Europe Region

In the Europe Region: A Member must include a provision in its contracts with a third party that performs services relating to Visa products and services that specifies that the third party must not:

- Misrepresent itself as being a Member
- Present itself to prospective Cardholders or Merchants under any trade name other than that registered with Visa

ID# 0029802	Edition: Apr 2020 | Last Updated: Oct 2016

10.2.4   Independent Sales Organizations – Europe Region

10.2.4.1   Requirements for Use of Independent Sales Organizations – Europe Region

In the Europe Region: A Member that contracts with an Independent Sales Organization must both:

- Ensure that the contract is limited to a maximum of 3 years. The Member may renew the contract.
- Not allow the Independent Sales Organization to perform any of the following functions:
  - Clearing and Settlement of Transactions
  - Payment to, or crediting of, Merchant accounts
  - Merchant or Cardholder account underwriting, activation, or charge-offs
  - Risk management, including Transaction monitoring
  - Approval and review of Merchants
  - Approval of Cardholder applications
  - Establishment of Merchant fees for Transactions

ID# 0029583	Edition: Apr 2020 | Last Updated: Oct 2016

10.3   Account and Transaction Information Security

10.3.1   Account, Cardholder, and Transaction Information Security

10.3.1.1   Requirement to Investigate Suspected or Confirmed Loss, Theft, Compromise, Fraud, or Laundering

A Member must comply with *What To Do If Compromised*[1] and conduct a thorough investigation of suspected or confirmed:

- Loss, theft, or compromise of Visa account or Cardholder information
- Loss, theft, or compromise of Visa account or Cardholder information by one of its agents or Merchants
- Fraud and/or laundering of a Transaction

After completing the investigation, the Member must demonstrate its ability to prevent future loss, theft, or compromise of Visa account or Cardholder information, as specified in the Account Information Security Program and *Payment Card Industry Data Security Standard (PCI DSS)*.

If Visa requires a Member or its agent to conduct an additional investigation, the Member or its agent must:

- Provide access to the premises involved in the investigation
- Provide Visa and its agent access to all applicable records, including, but not limited to, the following:
  - Computer forensic reports
  - Network diagrams
  - Systems connected directly or indirectly to VisaNet or used to transmit, process, or store account data
- Engage a forensic investigator approved by the Payment Card Industry Security Standards Council. If the Member or its agent fails to do so, Visa may engage an investigator to perform a forensic investigation and will assess all investigative costs to the Member.

[1] In the Europe Region: *What To Do If Compromised: Visa Europe Data Compromise Procedures*

ID# 0007123	Edition: Apr 2020	Last Updated: Apr 2017

10.3.1.2   Member Reporting of Loss or Theft of Information

As specified in *What To Do If Compromised*,[1] a Member must immediately report to Visa by telephone, fax, or email the suspected or confirmed:

- Loss, theft, or compromise of Visa account or Cardholder information[2]

- Loss, theft, or compromise of Visa account or Cardholder information by one of its agents or Merchants[2]

- Fraud and/or laundering of a Transaction

The report must contain, to the extent possible:

- Member and Merchant or agent name

- Format, number, and range of account information missing or compromised

- Specific Account Numbers missing or compromised

- Type or data elements of account information on missing material (for example: Track 1 data, Track 2 data, CVV2, Cardholder name, Cardholder address)

- Pertinent details about the loss, theft, or compromise and ensuing investigation

- Contact name and telephone number for additional information

- Name and telephone number of person reporting the loss or theft

[1] In the Europe Region: *What To Do If Compromised: Visa Europe Data Compromise Procedures*

[2] In the US Region: May be reported on behalf of a Member by its agent or by a Merchant or its agent

ID# 0007999	Edition: Apr 2020 | Last Updated: Apr 2017

10.3.1.3   Account Information Security Program Assessment – Europe Region

In the Europe Region: Visa may, at its discretion, require an Acquirer to undergo a formal Account Information Security Program assessment to validate compliance with the program, including Merchant- and Agent-reported Payment Card Industry Data Security Standard (PCI DSS) compliance levels. The Acquirer will be responsible for the reimbursement of any Visa-incurred expenses.

ID# 0029659	Edition: Apr 2020 | Last Updated: Oct 2019

10.3.1.4   Member Cooperation to Protect Against Data Compromise – Europe Region

In the Europe Region: A Member must cooperate with Visa to protect the Visa system and Members against data compromises of account information and Transaction Information. A Member that fails to do so may be subject to a non-compliance assessment of EUR 100,000.

Lack of Member cooperation is classified as:

- Failure to immediately disclose a suspected compromise to Visa

- Failure to distribute at-risk Account Numbers to Visa within 7 calendar days of notification of a suspected compromise

- Failure to notify law enforcement that a crime may have been committed

- Failure to engage, in writing, a PCI Forensic Investigation (PFI) within 10 business days of Notification of a suspected compromise

- Failure of a Member or Group Member to distribute to Visa all Transaction data processed during the window of exposure on a BIN or an Acquiring Identifier by the Member or Group Member (or by an at-risk entity on their behalf) within 15 calendar days of a Visa request

- Failure to identify at-risk Account Numbers

- Any other aspect regarding a Member's management of data compromises or that Visa deems to have an adverse impact on the Visa system

- Such Transaction data must be distributed to Visa irrespective of which entity processed this data.

- The at-risk entity and the window of exposure on a BIN or an Acquiring Identifier are defined by Visa on a case-by-case basis.

ID# 0029596	Edition: Apr 2020 | Last Updated: Oct 2019

10.3.1.5   Compromise at Member's Contractors or Agents – US Region

In the US Region: A Member must implement policies and procedures requiring its contractors or Agents to notify the Member if the contractor or Agent experiences a security breach or reasonably believes that Cardholder information was compromised as a result of that breach.

ID# 0001799	Edition: Apr 2020 | Last Updated: Oct 2014

10.3.1.6   Security Standards for Materials Containing Account Information – US Region

In the US Region: An Issuer must ensure that both a fulfillment vendor or prepaid storage facility that is used to consolidate materials containing account information before delivering them to the United States Postal Service or overnight courier comply with the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors*.

ID# 0008026	Edition: Apr 2020 | Last Updated: Oct 2014

10.3.2   Confidential Consumer Cardholder Information

10.3.2.1   Visa Safeguards for Confidential Consumer Cardholder Information – US Region

In the US Region: Visa and its subsidiaries will restrict access to Confidential Consumer Cardholder Information to those employees that Visa or its subsidiaries has determined need to know that information to provide products and services to Members.

Visa and its subsidiaries will maintain physical, electronic, and procedural safeguards that are designed to:

- Maintain the security and confidentiality of Confidential Consumer Cardholder Information
- Protect against anticipated threats or hazards to the security or integrity of Confidential Consumer Cardholder Information
- Prevent unauthorized access to, or use of, such Confidential Consumer Cardholder Information that could result in substantial harm or inconvenience to Consumer Cardholders

Visa will notify a Member in the event that Visa reasonably believes that Confidential Consumer Cardholder Information about a Member's customer has been compromised due to a breach of security.

| ID# 0008003 | Edition: Apr 2020 | Last Updated: Oct 2014 |

10.3.2.2   Destruction of Confidential Consumer Cardholder Information – US Region

In the US Region: Visa and its subsidiaries will use reasonable measures designed to ensure that all Confidential Consumer Cardholder Information is erased or destroyed, in accordance with regulatory guidelines, so as to render the information unreadable.

A Member must implement policies and procedures designed to ensure timely disposal or destruction of Confidential Consumer Cardholder Information, in accordance with regulatory guidelines, in a manner that makes the information unreadable.

| ID# 0008007 | Edition: Apr 2020 | Last Updated: Oct 2014 |

10.3.3   Data Protection – Europe Region

10.3.3.1   Data Protection Provisions – Europe Region

In the Europe Region: Depending on the service and as specified in the *Data Framework for Visa Services – Europe Region,* a Member must understand and accept that it is either:

- Both:

  – A data controller, as specified by European Data Protection legislation, with regard to all or certain Personal Data that the Member and/or Visa collects from Cardholders and Merchants with Visa and its subcontractors being the data processor

  – Primarily responsible for fulfilling all data protection responsibilities toward Cardholders and Merchants with whom it has a direct relationship

- Both:

  – A joint data controller together with Visa, as specified by European Data Protection legislation, with regard to all or certain Personal Data that the Member and/or Visa collects from Cardholders and Merchants with Visa and its subcontractors being the joint data controller

  – Jointly responsible with Visa for fulfilling all data protection responsibilities toward Cardholders and Merchants

ID# 0029585	Edition: Apr 2020 | Last Updated: Apr 2018

10.3.3.2   Data Protection Provisions – Member Responsibility as Sole Data Controller – Europe Region

In the Europe Region: If a Member is the sole data controller in respect of a service as specified in the *Data Framework for Visa Services – Europe Region,* it must do all of the following:

- Ensure that it complies fully with all applicable data protection laws with regard to Personal Data that it collects, stores, transfers, or otherwise processes

- Ensure that it has appropriate safeguards (such as binding corporate rules or standard contractual clauses) or any mechanism that is deemed legally adequate for making any data transfers outside the European Economic Area (EEA)

- Provide appropriate prior information to the Cardholder or Merchant about the intended processing of Personal Data by the Member and Visa

- Provide accurate data regarding its Cardholders to Visa, including informing Visa when Cardholder Personal Data must be corrected, updated, or deleted

- Respond promptly to a Cardholder or Merchant that contacts the Member seeking to exercise data protection rights and inform Visa of the response

- Adopt appropriate technical and organizational security measures for the storage and processing of such Personal Data, as more particularly specified in the relevant service description

- Ensure that Visa is permitted to transfer data outside the EEA and execute any required legal documentation on behalf of the data controller to adduce adequacy for the data transfer

- Work with the Cardholder or Merchant to resolve any dispute regarding Personal Data and inform Visa of the resolution

- Ensure that all staff are appropriately trained in line with their responsibilities under applicable data protection law

In addition, where the Member is located within the EEA and/or issues a Card to a Cardholder located within the EEA, it must, as sole data controller, do all of the following:

- Ensure that it is has a lawful basis for the processing of any Personal Data, including processing of any Personal Data by Visa

- Provide consent for Visa to engage sub-processors, including sub-processors located outside the EEA

- Notify Visa, following contact from any given regulatory authority in relation to data processed by Visa, unless applicable law prohibits such notification

- Determine a clear process for reporting and responding to Personal Data breaches and, in the event of a breach, notify the regulatory authority and data subjects where applicable

ID# 0029586   **Edition: Apr 2020 | Last Updated: Apr 2019**

10.3.3.3   Data Protection Provisions – Member and Visa Responsibilities as Joint Data Controllers – Europe Region

In the Europe Region: If a Member and Visa are joint data controllers in respect of a service, as specified in the *Data Framework for Visa Services – Europe Region,* each must do all of the following:

- Ensure that it complies fully with all applicable data protection laws with regard to Personal Data that it collects, stores, transfers, or otherwise processes

- Ensure that it has appropriate safeguards (such as binding corporate rules or standard contractual clauses) or any mechanism that is deemed legally adequate for making any data transfers outside the European Economic Area (EEA)

- Adopt appropriate technical and organizational security measures for the storage and processing of such Personal Data, as more particularly specified in the relevant service description

- Ensure that all staff are appropriately trained in line with their responsibilities

- All of the following:
  - Cooperate in response to any requests from a data protection authority
  - Respond promptly to a data subject that contacts Visa or the Member (as the case may be) seeking to exercise data subject rights and inform Visa or the Member (as the case may be) of the response

- – Assist Visa or the Member (as the case may be) in respect of responses to data subject requests

- – Work with the data subjects to resolve any issues regarding the processing of their Personal Data and inform Visa or the Member (as the case may be) of the response

A Member must both:

- Provide appropriate fair processing information to the data subjects about all of the intended processing of Personal Data by the Member and Visa

- Provide accurate data regarding its Cardholders to Visa, including promptly informing Visa when Cardholder Personal Data must be corrected, updated, or deleted

In addition, where a Member is located within the EEA and/or issues a Card to a Cardholder within the EEA, it must, as joint data controller, both:

- Appoint a contact point for all subject access requests and clearly communicate such details to data subjects

- Determine a clear process for reporting and responding to personal data breaches and, in the event of personal data breach, notify the regulatory authority and data subjects where applicable, after consultation with Visa

ID# 0029587	Edition: Apr 2020 | Last Updated: Apr 2019

10.3.3.4   Data Protection Provisions – Visa Responsibility as Data Processor – Europe Region

Visa will comply fully with all applicable European data protection laws in regard to the Personal Data it, or its sub-processor, stores and processes on behalf of its Members, as follows:

- Update the Personal Data of a Cardholder or Merchant when notified of such corrections or updates by a Member or Cardholder

- Assist a Member, where appropriate, with both technical and organizational support, to respond to a Cardholder or Merchant seeking to exercise data protection rights

- Respond to a Cardholder or Merchant that contacts Visa seeking to exercise data protection rights

- Delete, or, where applicable, return, any Personal Data at the end of the relevant retention period

- Adopt appropriate technical and organizational security measures, in line with associated risks and considering applicable costs, for the storage and processing of such Personal Data as disclosed by Members, as more particularly specified in the relevant service description

Visa Core Rules and Visa Product and Service Rules

- Work with a Member, Cardholder, or Merchant to resolve disputes raised to Visa regarding the processing of Personal Data

- To the extent that it is Visa's responsibility to do so, ensure that all transfers of Personal Data outside the European Economic Area (EEA) are on the basis of either:

  – An adequacy decision by the European Commission

  – Appropriate or suitable safeguards as required by applicable laws or regulations

Where Visa acts as a data processor, Visa will, for a Member that is located within the EEA and/or issues a Card to a Cardholder within the EEA, do all of the following:

- Include the subject matter, duration, and purpose of the processing, including the type of Personal Data involved and the categories of data subject, as specified in *Data Framework for Visa Services – Europe Region*

- Only process data on the instructions of the Member, unless otherwise required by European Law or Member State law. Where such processing takes place, Visa will notify the Member before undertaking such processing, unless applicable law prohibits such notification.

- Ensure that only authorized individuals under appropriate confidentiality terms have access to Personal Data

- Maintain technical and organizational measures to avoid unauthorized or unlawful processing of Personal Data and loss, destruction of, or damage to Personal Data. Such measures will be in line with associated risks and consider applicable costs.

- Ensure that, where Visa engages a sub-processor, the Member is notified of that engagement. All Visa obligations set out in this section will be passed onto that sub-processor. Visa will conduct a risk assessment and due diligence on that sub-processor. Visa will also give a Member a reasonable timeframe to object to the engagement of that sub-processor and the Member agrees and hereby consents for Visa to engage the relevant sub-processor where the Member fails to raise objections within the applicable timeframe. If the Member objects to the engagement of a sub-processor within the applicable timeframe, Visa may choose one of the following:

  – Decide not to use the sub-processor for that processing activity

  – Take the corrective steps requested by the Member in its objection (which remove the Member's objection) and proceed to use the sub-processor

  – Suspend or terminate the provision of the services that require use of the sub-processor

- Assist the Member in meeting any regulatory obligations in relation to data security, notification of personal data breaches, and data protection impact assessments

- Not disclose Personal Data without a Member's consent unless requested or authorized by that Member or required by European Union or Member State law. If required by law, Visa will consult with the Member to limit such disclosure.

- Provide the Member with all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulations

- Establish that a Member may conduct an audit on Visa in order to verify Visa's compliance with Visa's obligations under the General Data Protection Regulation and Visa's requirements as a data processor under the Visa Rules in relation to services that Visa provides to the Member, provided that:

  - The Member gives Visa reasonable notice in advance of any audit (where permitted by law).

  - The audit is carried out in a manner that causes the minimum possible disruption to Visa's business (including with respect to the length of the audit, the number and seniority of Visa personnel required to assist with the audit).

  - The Member and its third party auditor are subject to applicable Visa policies and confidentiality obligations.

  - The Member shall not be entitled to access records of any nature relating to any other Member.

- Notify the Member, without undue delay, of any Personal Data breach

- Notify the Member if, in Visa's opinion, a processing instruction from that Member infringes any applicable data protection regulation. In such an event, Visa will cease any processing activity in relation to that instruction

- Notify the relevant Member promptly if Visa is contacted by any given regulatory body, in relation to the processing of Personal Data. Visa will work with that Member in response to the regulatory body

- Notify the relevant Member promptly if Visa is contacted by any given data subject, in relation to the processing of Personal Data. Visa will assist that Member in response to the data subject

ID# 0029588	Edition: Apr 2020 | Last Updated: Apr 2019

10.3.3.5   Data Protection Provisions – Member Provision to Visa of Cardholder Data – Europe Region

In the Europe Region: A Member must do all of the following:

- Warrant that, as applicable, the terms and conditions of its Cardholder agreements do and will continue to permit Visa to conduct propensity modelling and to use such data to build and market products and services to third parties

- Ensure that all fair processing notices have been given to a Cardholder (and/or, as applicable, consents obtained from a Cardholder) and such notices are sufficient in scope to enable Visa to process any Cardholder personal data as required and in accordance with applicable laws or regulations, including ensuring that such fair processing notices comply with all other Cardholder agreement requirements

- Indemnify Visa for and against Claims and Liabilities arising out of or in connection with a breach of such warranty

ID# 0029589	Edition: Apr 2020	Last Updated: Apr 2018

10.3.3.6   Data Transfers out of the European Economic Area and Switzerland – Europe Region

In the Europe Region: Transfers of Personal Data out of the European Economic Area (EEA) and Switzerland, in connection with the services provided by Visa under the *Data Framework for Visa Services – Europe Region,* to any country that has not been deemed as "adequate" by the relevant data protection authority shall be governed by the *Data Transfer Framework – Europe Region.*

ID# 0030605	Edition: Apr 2020	Last Updated: Apr 2019

10.4   Activity and Compliance Monitoring

10.4.1   Member Activity Monitoring Requirements

10.4.1.1   Acquirer Investigation of Merchant Outlet

An Acquirer must investigate a Merchant Outlet that appears on an exception report.

If the investigation reveals Merchant involvement in illegal or fraudulent activity, the Acquirer must do all of the following:

- Take appropriate legal action to minimize losses
- Cooperate with Issuers and law enforcement agencies
- Attempt to make the Merchant responsible for the Transaction
- Hold funds, if possible
- Initiate criminal and civil proceedings against the Merchant, if applicable

ID# 0002419	Edition: Apr 2020	Last Updated: Oct 2016

10.4.1.3   Merchant Activity Monitoring and Reporting Requirements – Europe Region

In the Europe Region: An Acquirer must do all of the following:

- Retain at least the following daily data and use it to determine "normal daily activity" over a period of 30 days, beginning after each Merchant's initial Deposit:
  - Gross sales volume
  - Average Transaction amount
  - Number of Transaction Receipts
  - Average elapsed time between the Transaction Date of the Transaction Receipt and the Settlement Date (counting each as one day)
  - Number of Disputes
- Begin the daily monitoring of the Merchant's activity processed on the 31st calendar day from the first Deposit against the normal daily activity using an average of the data from the previous 30 days
- Compare current related data to the normal daily activity parameters at least daily
- At least weekly, review the Merchant's normal daily activity, using the previous week's activity
- At least monthly, adjust the Merchant's normal daily activity, using the previous month's activity

The Acquirer must generate an exception report on a daily basis and report to Visa within 2 business days if either:

- Any of the following exceeds 150% of normal daily activity:
  - Number of daily Deposits
  - Gross amount of daily Deposits
  - Average Transaction amount
  - Number of daily Disputes
- The average elapsed time between the Processing Date and either the Transaction Date or the Settlement Date for a Transaction (counting each as one day) exceeds 15 calendar days

ID# 0029658 | Edition: Apr 2020 | Last Updated: Apr 2018

10.4.1.4   Merchant Deposit Monitoring – Europe Region

In the Europe Region: An Acquirer that has been identified by the Fraud Monitoring Programs specified in *Section 10.4.4.1, Visa Acquirer Monitoring Program (VAMP),* must implement daily monitoring and produce exception reports in order to reduce their losses. Failure to implement

Visa Core Rules and Visa Product and Service Rules

effective monitoring may result in a non-compliance assessment of EUR 25,000 for each month in which actions remain outstanding.

Exception reports must be generated according to the parameters specified in *Table 10-1, Merchant Deposit Monitoring Parameters – Europe Region* where the respective defined thresholds have been exceeded.

In addition to daily monitoring, an Acquirer must employ adequate risk management resources to control and monitor its Merchants, and undertake specific investigative actions to combat any fraudulent activity.

A Merchant's normal daily trading and activity pattern must be adjusted on a daily basis, using the most recent activity and replacing the oldest data. Merchant trading averages must be calculated using a 90-day rolling average.

Table 10-1: Merchant Deposit Monitoring Parameters – Europe Region

Parameter	Exceeds	By
An individual Transaction value	The daily average Transaction value for the individual Merchant Outlet	% threshold defined by the Acquirer
The total number of Transactions deposited daily	The normal daily average number of Transactions for the individual Merchant Outlet	% threshold defined by the Acquirer
The total value of Transactions deposited daily	The normal daily average value deposited for the individual Merchant Outlet	% threshold defined by the Acquirer
The number and value of Transactions processed on the same Cardholder account in one or more Merchants	A threshold defined by the Acquirer	N/A
The number and value of incoming Retrieval Requests and Disputes processed	A predetermined ratio or threshold defined by the Acquirer	N/A
The daily total value of key-entered Transactions processed in a Merchant Outlet	Exceeds the normal daily average total of key-entered Transactions for the Merchant Outlet	% threshold defined by the Acquirer
The daily number of key-entered	Exceeds the normal daily average	% threshold defined by the

Table 10-1: Merchant Deposit Monitoring Parameters – Europe Region (continued)

Parameter	Exceeds	By
Transactions processed in a Merchant Outlet	number of key-entered Transactions for the Merchant Outlet	Acquirer
The percentage of Transactions processed below a Merchant's Floor Limit	The normal daily average number of Transactions below the Merchant's Floor Limit	% threshold defined by the Acquirer
The total number and value of Transactions on the same BIN at the same Merchant Outlet on the same day	A threshold defined by the Acquirer	N/A
The value of credits (refunds) processed	The normal daily average value of credits for the individual Merchant Outlet	A threshold defined by the Acquirer
The number of credits (refunds) processed	The normal daily average number of credits for the individual Merchant Outlet	A threshold defined by the Acquirer
A deposit is received from a Merchant that has not processed any Transaction activity in a specified period	N/A	Within the last 3 months or by a time period specified by the Acquirer
A deposit is processed for a Merchant after the Merchant Agreement was terminated	N/A	N/A

If Visa determines that:

- The parameters defined in _Table 10-1, Merchant Deposit Monitoring Parameters – Europe Region_ do not allow sufficient detection of fraud, then Visa may, at its discretion, vary or impose new parameters to identify changing fraud patterns
- The thresholds defined by the Acquirer do not allow sufficient detection of fraud, then Visa may, at its discretion, impose a threshold value on the Acquirer

ID# 0029811   **Edition: Apr 2020 | Last Updated: Oct 2019**

10.4.1.5   Acquirer Provision of Fraud Advice Reports – Europe Region

In the Europe Region: An Acquirer must provide its Merchant with fraud advice reports upon Merchant request.

ID# 0029599	Edition: Apr 2020	Last Updated: Oct 2016

10.4.1.6   Merchant Exception Reports – US Region

In the US Region: Beginning with Merchant Outlet Deposit activity processed on the 31st calendar day from the first Deposit, an Acquirer must generate unusual activity reports if either of the following occurs:

- Current weekly gross sales volume equals or exceeds USD 5,000 and any of the following meets or exceeds 150% of normal weekly activity:
  - Number of weekly Transaction Deposits
  - Gross amount of weekly Deposits
  - Average Transaction amount
  - Number of weekly Disputes
- Average elapsed time between the Transaction Date and the Acquirer's Processing Date for a Transaction (counting each as one day) exceeds 15 calendar days

ID# 0002223	Edition: Apr 2020	Last Updated: Apr 2018

10.4.2   Monitoring of Visa Compliance

10.4.2.1   Member Monitoring of Visa Compliance – US Region

In the US Region: Visa and its subsidiaries will adopt policies and procedures and provide Members with appropriate reviews and reports to enable Members to monitor the compliance of Visa and its subsidiaries with these commitments.

ID# 0000512	Edition: Apr 2020	Last Updated: Oct 2014

10.4.3   Dispute Monitoring

10.4.3.1   Visa Dispute Monitoring Program (VDMP)

Visa monitors Merchant Outlets that generate an excessive level of Disputes through the Visa Dispute Monitoring Program (VDMP).

Visa will identify a Merchant Outlet under the VDMP standard program if it meets or exceeds both of the following monthly standard program thresholds:

- 100 Dispute count

- 0.9% ratio of Disputes-to-sales Transaction count

Visa will monitor a Merchant Outlet identified in the VDMP under the high-risk program for any of the following reasons:

- The Merchant exceeds the standard program thresholds and is categorized or should be categorized by a high-brand risk MCC, as specified in *Section 10.4.6.1, High-Brand Risk Merchants.*

- For Merchants that are not and should not be categorized by a high-brand risk MCC, the Merchant meets or exceeds the VDMP monthly excessive Dispute threshold of both:

  - 1,000 Dispute count

  - 1.8% of Disputes-to-sales Transaction count

- Visa determines that the Merchant caused undue harm to the goodwill of the Visa payment system.

- The Merchant's Acquirer is subject to risk reduction measures, as specified in *Section 1.10.1.2, Member Risk Reduction Requirements,* for poor Merchant management practices.

Visa may modify or create new monthly VDMP performance levels.

Monitoring includes all Dispute conditions except Dispute Condition 10.5: Visa Fraud Monitoring Program.

Except for certain markets,[1] only International Transactions are included in VDMP monitoring.

A Merchant that is moved from the VDMP standard program to the VDMP high-risk program because it exceeded the excessive Dispute threshold will continue to be monitored under the VDMP high-risk program until the Merchant exits the VDMP.

A Merchant that is monitored in the VDMP high-risk program because it exceeded the excessive Dispute threshold will not be moved to the VDMP standard program, regardless of whether its performance drops below the monthly excessive Dispute threshold.

A Merchant that changes Acquirers and/or countries while identified in the VDMP will be assigned the equivalent program status with the new Acquirer and/or country if the Merchant has not exited the program.

Visa may require the Acquirer or its Merchant to deploy appropriate Dispute or fraud remediation tools or technologies to address unusual activity in the individual cases identified through the VDMP.

A Merchant Outlet will exit the VDMP if it is below the program thresholds for 3 consecutive months.

For VDMP compliance purposes, Visa will include only the first 10 Disputes per calendar month, for each Payment Credential at each Merchant Outlet.

[1] Program monitoring includes Domestic Transactions and International Transactions for all of the following: AP Region (Australia), Canada Region, Europe Region (Germany, United Kingdom), LAC Region (Brazil), and US Region. Visa may modify this list of markets.

ID# 0029283	Edition: Apr 2020 | Last Updated: Apr 2020

10.4.3.2   Visa Dispute Monitoring Program (VDMP) Timelines

An Acquirer must comply with *Table 10-2, VDMP Standard Program Timeline,* or *Table 10-3, VDMP High-Risk Program Timeline* as applicable.

Visa may escalate a Merchant Outlet that causes undue harm to the Visa payment system to the VDMP high-risk program timeline.

Table 10-2: VDMP Standard Program Timeline

Program Status	Acquirer Actions
Program Month 1 Notification	• Within 10 calendar days of receipt of Notification that a Merchant Outlet has met or exceeded the thresholds, the Acquirer must do all of the following: – Notify the Merchant – Review Merchant activity and research the cause of the excessive Disputes – Provide Visa with the specific information requested
Program Month 2 – 4 Workout Period	• Month 2: within 10 calendar days of date on the Notification, submit to Visa all of the following: – Acceptable Dispute remediation plan – Copy of Merchant application, if requested – Copy of Merchant contract, if requested • From month 2 onwards: implement a Dispute remediation plan • From month 3 onwards: within 10 calendar days of the date on the Notification, provide to Visa written updates to the Dispute remediation plan

Visa Product and Service Rules

10 Risk

Visa Core Rules and Visa Product and Service Rules

Table 10-2: VDMP Standard Program Timeline (continued)

Program Status	Acquirer Actions
Program Month 5 – 11 Enforcement Period	- From month 5 onwards: – Fees are applicable – Continue working with Merchant to ensure that the Dispute remediation plan is fully implemented and is effectively reducing Disputes – Adjust the Dispute remediation plan as required and provide updates to Visa - Month 8: provide Visa with written confirmation that the Merchant has been notified that it may lose Visa acceptance privileges if it fails to reduce its Disputes below the program thresholds by month 12 - From month 10 onwards: review fees are applicable
Program Month 12 Enforcement Period (and, in the Europe Region subsequent months)	- Non-compliance assessments and fees are applicable - Review fees are applicable - Merchant Outlet is eligible for disqualification - Continue to implement and provide to Visa the reduction plan, adjusting it as necessary to effectively reduce Disputes

Table 10-3: VDMP High-Risk Program Timeline

Program Status	Acquirer Actions
Program Month 1 Enforcement Period	- Non-compliance assessments and fees are applicable - Review Merchant activity and determine the cause of the excessive Disputes - Within 10 calendar days of receipt of Notification that a Merchant Outlet has met or exceeded the thresholds, the Acquirer must both: – Notify the Merchant – Provide Visa with the specific information requested and an acceptable Dispute remediation plan
Program Month 2 – 5 Enforcement Period	- Non-compliance assessments and fees are applicable - Work with Merchant to ensure that the Dispute remediation plan is fully implemented and is effectively reducing Disputes - Provide to Visa a written monthly status on the Acquirer's progress to

Table 10-3: VDMP High-Risk Program Timeline (continued)

Program Status	Acquirer Actions
	reduce the Merchant's Disputes
Program Month 6 – 11 Enforcement Period	• Non-compliance assessments and fees are applicable • Provide written monthly status to Visa on the Acquirer's progress to reduce the Merchant's Disputes • Month 6: provide Visa with a copy of the Acquirer's notification to the Merchant that excessive Disputes may lead to disqualification • From month 7 and onwards: review fees are applicable
Program Month 12 Enforcement Period (and, in the Europe Region, subsequent months)	• Non-compliance assessments and fees are applicable • Review fees are applicable • Merchant Outlet is eligible for disqualification • Continue to implement and provide to Visa the reduction plan, adjusting it as necessary to effectively reduce Disputes

ID# 0029284   Edition: Apr 2020 | Last Updated: Oct 2019

10.4.3.3   Visa Dispute Monitoring Program (VDMP) – Data Quality Compliance

If Visa determines that an Acquirer, its Third Party Agent, or its Merchant changed, modified, or altered the Merchant name or Merchant data in any way to circumvent the Visa Dispute Monitoring Program (VDMP), Visa may do either or both of the following:

• Assess a non-compliance assessment per Merchant Outlet per month to the Acquirer

• Permanently disqualify the Merchant and its principals from participating in the Visa Program

If an Acquirer submits Interchange for a single Merchant Outlet under multiple Merchant descriptors or Merchant accounts, Visa may:

• Consolidate the individual Merchant descriptors or Merchant accounts for monitoring purposes

• Notify the Acquirer of the aggregation and any potential non-compliance assessments

• Apply the program thresholds to the consolidated Merchant Outlet performance

• Track and report the consolidated Merchant activity

Visa may evaluate Payment Facilitator performance at the Sponsored Merchant level or by aggregating all Interchange activity.

ID# 0029285	Edition: Apr 2020	Last Updated: Oct 2019

10.4.3.4   Merchant Dispute Activity Monitoring – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: An Acquirer must monitor the Dispute-to-Interchange volume ratio of its Merchant and identify a Merchant that experiences all of the following activity levels during any month:

- 100 or more Interchange Transactions
- 100 or more Disputes
- A 1% or higher ratio of overall Dispute-to-Interchange volume

ID# 0002220	Edition: Apr 2020	Last Updated: Apr 2018

10.4.4   Acquirer Dispute and Fraud Monitoring

10.4.4.1   Visa Acquirer Monitoring Program (VAMP)

Visa monitors Acquirers that generate an excessive level of Disputes or Fraud Activity through the Visa Acquirer Monitoring Program (VAMP). Visa will identify an Acquirer if it meets or exceeds any of the following monthly thresholds for either excessive Disputes or Fraud Activity:

- Dispute Monitoring:
  - 750 Dispute count
  - 0.75% ratio of Disputes-to-sales Transaction count
- Fraud Activity Monitoring:
  - USD 500,000 fraud dollar amount
  - 0.75% ratio of fraud-dollar-to-sales-dollar amount
- In the US Region: For domestic Visa Secure Fraud Activity Monitoring, both:
  - USD 100,000 fraud dollar amount
  - 0.75% ratio of fraud-dollar-to-sales-dollar amount

Visa may modify or create new monthly VAMP performance levels.

Program monitoring includes all Disputes or Fraud Activity submitted by Issuers in the preceding calendar month and all sales Transactions submitted by the Acquirer in the preceding calendar month.

Except for certain markets,[1] only International Transactions are included in VAMP monitoring.

Visa may require the Acquirer or its Merchant to deploy appropriate Dispute or fraud remediation tools or technologies to address unusual activity in the individual cases identified through the VAMP.

An Acquirer will exit the VAMP if it is below the program thresholds for 3 consecutive months.

Visa may impose conditions on an Acquirer that knowingly acts to circumvent monitoring.

For VAMP compliance purposes, Visa will do all of the following:

- Include only the first 10 Disputes per calendar month, for each Payment Credential at each Merchant Outlet
- Include only the first 10 fraud Transactions reported to Visa per calendar month, for each Payment Credential at each Merchant Outlet
- Exclude fraud type code 3 (fraudulent application)

[1] Program monitoring includes Domestic Transactions and International Transactions for all the following: AP Region (Australia), Canada Region, Europe Region (Germany, United Kingdom), LAC Region (Brazil), US Region. Visa may modify this list of markets.

ID# 0029286   **Edition: Apr 2020 | Last Updated: Apr 2020**

10.4.4.2   Visa Acquirer Monitoring Program (VAMP) Timeline

An Acquirer that is identified in the Visa Acquirer Monitoring Program (VAMP) by exceeding VAMP thresholds must comply with *Table 10-4, VAMP Timeline*.

Table 10-4: VAMP Timeline

Program Status	Acquirer Actions

Month 1
Enforcement Period
	- Non-compliance assessments apply
	- Review portfolio activity and determine the cause of the excessive Disputes or Fraud Activity
	- Within 10 calendar days of the date on the Notification, submit to Visa both:
	  – Acceptable Dispute/Fraud Activity remediation plan
	  – Any documentation requested by Visa

Table 10-4: VAMP Timeline (continued)

Program Status	Acquirer Actions
Month 2 – 11 Enforcement Period	• Non-compliance assessments apply • Implement a Dispute/Fraud Activity remediation plan • Provide to Visa a written monthly status on the Acquirer's progress to reduce the portfolio's Dispute/Fraud Activity
Month 12 Enforcement Period (and, in the Europe Region, subsequent months)	• Non-compliance assessments apply • Continue to Implement and submit to Visa remediation plans to bring performance to within acceptable levels, as defined by the program thresholds • Visa may disqualify the Acquirer • If received from Visa, communicate any pending terminations to the Merchant(s) /Third Party Agent(s) • Provide to Visa a final, written recap of portfolio's performance and Dispute/Fraud Activity remediation initiatives

ID# 0029287   Edition: Apr 2020 | Last Updated: Oct 2018

10.4.5   Merchant Fraud Monitoring

10.4.5.1   Visa Fraud Monitoring Program (VFMP)

Visa monitors Merchant Outlets that generate an excessive level of fraud through the Visa Fraud Monitoring Program (VFMP).

Visa will identify a Merchant Outlet under the VFMP standard program if it meets or exceeds any of the following monthly program thresholds:

- Both:
  - USD 75,000 fraud amount
  - 0.9% fraud-dollar-to-sales-dollar ratio
- **Effective through 31 October 2020** In the US Region: For domestic counterfeit Automated Fuel Dispenser Transactions, both:

- USD 10,000 in US Issuer-reported counterfeit fraud in the previous calendar month
- 0.20% counterfeit fraud-dollar-to-sales-dollar ratio in the previous calendar month
- In the US Region: For domestic Visa Secure Transactions, both:
  - USD 7,500 in US Issuer-reported fraud in the previous calendar month
  - 0.75% fraud-dollar-to-sales-dollar ratio in the previous calendar month

Visa will monitor a Merchant Outlet identified in the VFMP under the high-risk program for any of the following reasons:

- The Merchant is categorized, or should be categorized, by a high-brand risk MCC, as specified in *Section 10.4.6.1, High-Brand Risk Merchants.*
- For Merchants that are not and should not be categorized by a high-brand risk MCC, the Merchant meets or exceeds the VFMP monthly excessive fraud threshold of either:
  - Both
    - USD 250,000 fraud amount
    - 1.8% fraud-dollar-to-sales-dollar ratio
  - **Effective through 31 October 2020** In the US Region: For domestic counterfeit Automated Fuel Dispenser Transactions, both:
    - USD 10,000 in Issuer-reported domestic counterfeit fraud in the previous calendar month
    - 2% counterfeit fraud-dollar-to-sales-dollar ratio in the previous calendar month
- Visa determines that the Merchant caused undue harm to the goodwill of the Visa payment system.
- The Merchant's Acquirer is subject to risk reduction measures, as specified in *Section 1.10.1.2, Member Risk Reduction Requirements,* for poor Merchant management practices.

Visa may modify or create new VFMP monthly performance levels.

Except for certain markets,[1] only International Transactions are included in VFMP monitoring.

A Merchant that is moved from the VFMP standard program to the VFMP high-risk program because it exceeded the excessive fraud threshold will continue to be monitored under the VFMP high-risk program until the Merchant exits the VFMP.

A Merchant that is monitored in the VFMP high-risk program because it exceeded the excessive fraud threshold will not be moved to the VFMP standard program, regardless of whether its performance drops below the monthly excessive fraud threshold.

A Merchant that changes Acquirers and/or countries while identified in the VFMP will be assigned the equivalent program status with the new Acquirer and/or country if the Merchant has not exited the program.

Visa may require the Acquirer or its Merchant to deploy appropriate fraud remediation tools or technologies to address unusual activity in the individual cases identified through the VFMP.

A Merchant Outlet will exit the VFMP if it is below the program thresholds for 3 consecutive months.

For VFMP compliance purposes Visa will both:

- Include only the first 10 fraud Transactions reported to Visa per calendar month, for each Payment Credential at each Merchant Outlet
- Exclude fraud type code 3 (fraudulent application)

In the Europe Region: If a Merchant has met or exceeded specified fraud performance thresholds, the Acquirer must work with the Merchant until the Merchant's fraud levels fall below the fraud performance thresholds.

[1] Program monitoring includes Domestic Transactions and International Transactions for all the following: AP Region (Australia), Canada Region, Europe Region (Germany, United Kingdom), LAC Region (Brazil), and US Region. Visa may modify this list of markets.

ID# 0029288	Edition: Apr 2020	Last Updated: Apr 2020

10.4.5.2   Visa Fraud Monitoring Program (VFMP) Timelines

An Acquirer must comply with *Table 10-5, VFMP Standard Program Timeline* and *Table 10-6, VFMP High-Risk Program Timeline,* as applicable.

Visa may escalate a Merchant Outlet that causes undue harm to the Visa payment system to the VFMP high-risk program timeline.

Table 10-5: VFMP Standard Program Timeline

Program Status	Acquirer Actions	Visa Secure Participant Acquirer Actions – US Region
Program Month 1 – Notification	Within 10 calendar days of receipt of Notification that a Merchant Outlet has met or exceeded the thresholds, the Acquirer must both: – Notify the Merchant – Provide Visa with the specific	• Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to all Visa Secure fraud Transactions associated with the current Merchant identification • Within 10 calendar days of receipt of

Table 10-5: VFMP Standard Program Timeline (continued)

Program Status	Acquirer Actions	Visa Secure Participant Acquirer Actions – US Region
	information requested • Review Merchant activity and research the cause of the excessive fraud	Notification that a Merchant Outlet has met or exceeded the thresholds, an Acquirer must do all of the following: – Notify the Merchant – Review Merchant activity and research the cause of the excessive fraud – Provide Visa with the specific information requested and an acceptable fraud remediation plan that includes implementation of standard e-Commerce risk management tools
Program Month 2 – 4 – Workout Period	• Month 2: submit all of the following to Visa within 10 calendar days of date on the Notification: – Acceptable fraud remediation plan – Copy of Merchant application, if requested – Copy of Merchant contract, if requested • From month 2 onwards: implement a fraud remediation plan • From month 3 onwards: provide written updates to the fraud remediation plan within 10 calendar days of the date on the Notification	• Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to all Visa Secure fraud Transactions associated with the current Merchant identification • Work with Merchant to ensure that the fraud remediation plan is fully implemented and is effectively reducing fraud • Provide written monthly status to Visa on the Acquirer's progress to reduce the Merchant's fraud
Program Month 5 – 11 – Enforcement Period	• From month 5 onwards: – Continue working with the Merchant to ensure that the fraud remediation plan is fully implemented and is effectively reducing fraud	• Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to all Visa Secure fraud Transactions associated with the current Merchant identification

Table 10-5: VFMP Standard Program Timeline (continued)

Program Status	Acquirer Actions	Visa Secure Participant Acquirer Actions – US Region
	– Adjust the fraud remediation plan as required and provide updates to Visa – Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to the fraud Transactions associated with the current Merchant identification • Month 8: provide Visa with written confirmation that the Merchant has been notified that it may lose Visa acceptance privileges if it fails to reduce its fraud below the program thresholds by month 12	• Provide written monthly status to Visa on Acquirer's progress to reduce the Merchant's fraud • Month 6: provide Visa with a copy of the Acquirer's notification to the Merchant that excessive fraud may lead to disqualification
Program Month 12 – Enforcement Period (and, in the Europe Region, subsequent months)	• Merchant Outlet is eligible for disqualification • Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to the fraud Transactions associated with the current Merchant identification • Continue to implement and submit to Visa the fraud remediation plan, adjusting as necessary to effectively reduce fraud	• Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to all Visa Secure fraud Transactions associated with the current Merchant identification • Merchant Outlet is eligible for disqualification

Table 10-6: VFMP High-Risk Program Timeline

Program Status	Acquirer Responsibility
Program Month 1 – Enforcement Period	• Non-compliance assessments are applicable[1] • Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to the fraud Transactions associated with the current Merchant identification • Within 10 calendar days of receipt of Notification that a Merchant Outlet has met or exceeded the thresholds, an Acquirer must do all of the following: – Notify the Merchant

Table 10-6: VFMP High-Risk Program Timeline (continued)

Program Status	Acquirer Responsibility
	– Review Merchant activity and research the cause of the excessive fraud – Provide Visa with the specific information requested and an acceptable fraud remediation plan
Program Month 2 – 5 – Enforcement Period	• Non-compliance assessments are applicable[1] • Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to the fraud Transactions associated with the current Merchant identification • Work with Merchant to ensure that the fraud remediation plan is fully implemented and is effectively reducing fraud • Provide written monthly status to Visa on the Acquirer's progress to reduce the Merchant's fraud
Program Month 6 – 11 – Enforcement Period	• Non-compliance assessments are applicable[1] • Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to the fraud Transactions associated with the current Merchant identification • Provide written monthly status to Visa on the Acquirer's progress to reduce the Merchant's fraud • Month 6: provide Visa with a copy of the Acquirer's notification to the Merchant that excessive fraud may lead to disqualification
Program Month 12 – Enforcement Period (and, in the Europe Region, subsequent months)	• Non-compliance assessments are applicable[1] • Dispute Condition 10.5: Visa Fraud Monitoring Program liability is applicable to the fraud Transactions associated with the current Merchant identification • Merchant Outlet is eligible for disqualification • Continue to provide written updates to Visa, with information about the plan's effectiveness in reducing fraud levels

[1] **Effective through 31 October 2020** In the US Region: Does not apply to US domestic counterfeit Automated Fuel Dispenser Transactions.

ID# 0029289   **Edition: Apr 2020 | Last Updated: Apr 2019**

10.4.5.3   Visa Fraud Monitoring Program (VFMP) – Data Quality Compliance

If Visa determines that an Acquirer, its Third Party Agent, or its Merchant changed, modified, or altered the Merchant name or Merchant data in any way to circumvent the Visa Fraud Monitoring Program (VFMP), Visa may do either or both of the following:

- Assess a non-compliance assessment per Merchant Outlet per month to the Acquirer

- Permanently disqualify the Merchant and its principals from participating in the Visa Program

If an Acquirer submits Interchange for a single Merchant Outlet under multiple Merchant descriptors or Merchant accounts, Visa may:

- Consolidate the individual Merchant descriptors or Merchant accounts for monitoring purposes

- Notify the Acquirer of the aggregation and any potential non-compliance assessments

- Apply the program thresholds to the consolidated Merchant Outlet performance

- Track and report the consolidated Merchant activity

Visa may evaluate Payment Facilitator performance at the Sponsored Merchant level or by aggregating all Interchange activity.

ID# 0029290   **Edition: Apr 2020 | Last Updated: Oct 2016**

10.4.5.4   Acquirer Control of Force Post Transactions

An Acquirer must do all of the following if it has a Merchant or Sponsored Merchant enabled with force post[1] functionality:

- Conduct an enhanced due diligence review of the Merchant or Sponsored Merchant, as specified in the *Visa Global Acquirer Risk Standards*

- Validate and document that the Merchant or Sponsored Merchant has a legitimate business case to submit force post Transactions into Interchange

- Ensure risk controls are implemented to restrict the Merchant or Sponsored Merchant's ability to submit fraudulent Transactions into Interchange

Acquirers that fail to comply with this requirement resulting in the material, artificial manipulation of the clearing position for either a Merchant or Visa Card account[2], may be subject to non-compliance assessments, as specified in *Section 1.12.2.8, Willful or Significant Violations Schedules*

Acquirers may be subject to all costs associated with reversing the position(s) created by force post activity.

This does not apply to below-Floor Limit Transactions.

¹ Force Post functionality enables a Merchant to submit Clearing Record(s) with a manually entered Authorization Code.

² Force Post fraud involves Clearing Record(s) processed with either a fictitious, or no Authorization Code.

ID# 0030120	Edition: Apr 2020	Last Updated: Apr 2018

10.4.5.5   Card-Absent Merchant Requirement to Validate Cardholder Approval

Effective 18 April 2020 in the AP Region, Canada Region, Europe Region, LAC Region, US Region, and effective 1 July 2020 in the CEMEA Region An Acquirer must ensure that its Card-Absent Environment Merchant sets daily limits after which the Merchant must perform additional verification to confirm that the Cardholder approves continued spend. These limits must be appropriate for the Merchant business but must not exceed 25 Transactions in one day.

ID# 0030641	Edition: Apr 2020	Last Updated: Apr 2020

10.4.5.6   Merchant Withdrawal of Services or Asset Following a Fraud Dispute

Effective 18 April 2020 in the AP Region, Canada Region, Europe Region, LAC Region, US Region, and effective 1 July 2020 in the CEMEA Region An Acquirer must ensure that its Merchant attempts to revoke provision of goods or services from the Cardholder after a Dispute Category 10 (Fraud) Dispute and that the Merchant has a process in place to prevent reoccurrence by the Cardholder.

If the fraud is due to a Cardholder account with a Merchant being taken over, the Merchant must re-authenticate the Cardholder before any additional Authorization Requests.

ID# 0030642	Edition: Apr 2020	Last Updated: Apr 2020

10.4.6   High-Brand Risk Activity

10.4.6.1   High-Brand Risk Merchants

Effective through 16 October 2020 A Merchant required to use one of the following MCCs is considered a High-Brand Risk Merchant:

- 5962 (Direct Marketing – Travel-Related Arrangement Services)
- 5966 (Direct Marketing – Outbound Telemarketing Merchants)
- 5967 (Direct Marketing – Inbound Telemarketing Merchants)
- 7995 (Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks)
- 5912 (Drug Stores, Pharmacies)

- 5122 (Drugs, Drug Proprietaries, Druggist Sundries)
- 5993 (Cigar Stores and Stands), for Merchants that sell cigarettes in a Card-Absent Environment

Effective 17 October 2020 Visa classifies a Card-Absent Environment Merchant required to use any of the following MCCs as a High-Brand Risk Merchant:

- For all Card-Absent Transactions using the following MCCs:
  - 5122 (Drugs, Drug Proprietaries, Druggist Sundries)[1]
  - 5912 (Drug Stores, Pharmacies)[1]
  - 5962 (Direct Marketing – Travel-Related Arrangement Services)
  - 5966 (Direct Marketing – Outbound Telemarketing Merchants
  - 5967 (Direct Marketing – Inbound Telemarketing Merchants)
  - 5993 (Cigar Stores and Stands)[1]
  - 7273 (Dating and Escort Services)
  - 7995 (Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks)
- For certain Card-Absent Transactions using the following MCCs:
  - 4816 (Computer Network/Information Services), for the sale of access to cyberlockers or remote digital file-sharing services
  - 5816 (Digital Goods – Games), for Transactions involving skilled game wagering (for example: daily fantasy sports)
  - 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [Not Money Transfer], Travelers Cheques, and Debt Repayment), for the sale of cryptocurrencies

[1] In the AP Region, Canada Region, CEMEA Region, Europe Region, LAC Region: Applies only if the Merchant conducts Transactions other than Domestic Transactions

ID# 0008137   **Edition: Apr 2020 | Last Updated: Apr 2020**

10.4.7   High-Brand Risk Activity

10.4.7.1   Acquirer Monitoring of Payment Facilitators and High-Brand Risk Merchants

For a High-Risk Internet Payment Facilitator or High-Brand Risk Merchant, an Acquirer must do all of the following:

- Retain at least the following daily data:
  - Gross sales volume
  - Average Transaction amount
  - Number of Transaction Receipts
  - Number of Disputes
- Collect the data over a period of at least one month, beginning after each Merchant's initial Deposit
- Use the data to determine the Merchant's normal daily activity of the categories specified in this section
- Begin the daily monitoring of the Merchant's activity processed on the 31st calendar day from the first Deposit
- Compare current related data to the normal daily activity parameters at least daily
- Review the Merchant's normal daily activity at least weekly, using the previous week's activity
- At least monthly, adjust the Merchant's normal daily activity, using the previous month's activity

Upon Visa request, an Acquirer must provide all of the following within 7 calendar days to demonstrate compliance with High-Brand Risk Merchant monitoring standards:

- Original Merchant underwriting package
- Copies of actual reports or records used to monitor the Merchant's Deposits
- Any other data requested by Visa

ID# 0026340	Edition: Apr 2020 | Last Updated: Apr 2020

10.4.7.2   High-Brand Risk Merchant Exception Reports

An Acquirer must generate High-Brand Risk Merchant exception reports daily if either:

- The Merchant's current weekly gross sales volume equals or exceeds USD 10,000 (or local currency equivalent), and any of the following exceeds 150% of the Merchant's normal daily activity:
  - Number of daily Transaction Deposits
  - Gross amount of daily Deposits
  - Average Transaction amount
  - Number of daily Disputes

- The average elapsed time between the Transaction Date and Processing Date or between the Processing Date and Settlement Date for a Transaction (counting each as one day respectively) exceeds 15 calendar days

The Acquirer must investigate a Merchant that appears on its High-Brand Risk Merchant exception report within one business day of generating the report. If the investigation reveals Merchant involvement in illegal or fraudulent activity, the Acquirer must do all of the following:

- Take appropriate legal action to minimize losses
- Cooperate with Issuers and law enforcement agencies
- Attempt to make the Merchant responsible for the Transaction
- Hold funds, if possible
- Initiate criminal and civil proceedings against the Merchant, if applicable

ID# 0026341	Edition: Apr 2020 | Last Updated: Apr 2020

10.4.7.3   Requirements for High Brand-Risk Merchants and High Brand-Risk Sponsored Merchants

Visa may impose security or authentication requirements on a Merchant that it considers to be a High Brand-Risk Merchant or a High Brand-Risk Sponsored Merchant.

ID# 0029660	Edition: Apr 2020 | Last Updated: Apr 2020

10.4.7.4   Merchant Disqualification from the Visa Program

Effective through 16 October 2020 In the US Region: Visa may disqualify a Merchant specified in *Section 10.4.6.1, High-Brand Risk Merchants,* from participating in the Visa Program if the Merchant does any of the following:

- Meets or exceeds a critical level of Dispute activity
- Acts with the intent to circumvent Visa programs
- Causes harm to the Visa system

Visa will send a Notification to the Acquirer advising all of the following:

- The date the Acquirer must stop submitting the disqualified Merchant's Transactions
- Reasons for the disqualification
- Notice of the right to appeal

The Acquirer may appeal the disqualification as follows:

- The Acquirer's appeal letter must be received by Visa within 15 days of the Acquirer's receipt of the disqualification Notification.

- The Acquirer must pay a non-refundable fee and include it with the appeal letter.

- The evidence and arguments for the appeal must be submitted in the appeal letter.

- No oral presentations are permitted.

Effective 17 October 2020 Visa may disqualify a Merchant specified in *Section 10.4.6.1, High-Brand Risk Merchants,* from participating in the Visa Program if the Merchant does any of the following:

- Meets or exceeds a critical level of Dispute activity

- Acts with the intent to circumvent Visa programs

- Causes harm to the Visa system

Visa will send a Notification to the Acquirer advising all of the following:

- The date the Acquirer must stop submitting the disqualified Merchant's Transactions

- Reasons for the disqualification

- Notice of the right to appeal

The Acquirer may appeal the disqualification as follows:

- The Acquirer's appeal letter must be received by Visa within 15 days of the Acquirer's receipt of the disqualification Notification.

- The Acquirer must pay a non-refundable fee and include it with the appeal letter.

- The evidence and arguments for the appeal must be submitted in the appeal letter.

- No oral presentations are permitted.

| ID# 0005865 | Edition: Apr 2020 | Last Updated: Apr 2020 |

10.4.8   High-Risk Internet Payment Facilitator Requirements

10.4.8.1   High-Risk Internet Payment Facilitator Agreement

An Acquirer must ensure that a High-Risk Internet Payment Facilitator Agreement requires both:

- That the High-Brand Risk Sponsored Merchant Agreement be signed by a senior officer of the High-Risk Internet Payment Facilitator

- The High-Risk Internet Payment Facilitator to report both:
  – Acquisition of new High-Brand Risk Sponsored Merchants
  – Monthly Transaction activity for all High-Brand Risk Sponsored Merchants.

ID# 0026332	Edition: Apr 2020	Last Updated: Apr 2020

10.4.8.2   Visa Right to Prohibit or Disqualify Sponsored Merchants

Effective through 16 October 2020 In the US Region: Visa may require an Acquirer to directly contract with a Sponsored Merchant if the Sponsored Merchant either:

- Generates or has a history of generating excessive levels of exception items (Disputes and/or credits) within a 12-month period
- Takes action to evade responsibility for compliance with the Visa Rules

Visa may disqualify a High-Risk Internet Payment Facilitator or High-Brand Risk Sponsored Merchant in accordance with the Visa Dispute Monitoring Program or for other activity that causes undue harm to the Visa system.

Effective 17 October 2020 Visa may require an Acquirer to directly contract with a Sponsored Merchant if the Sponsored Merchant either:

- Generates or has a history of generating excessive levels of exception items (Disputes and/or credits) within a 12-month period
- Takes action to evade responsibility for compliance with the Visa Rules

Visa may disqualify a High-Risk Internet Payment Facilitator or High-Brand Risk Sponsored Merchant in accordance with the Visa Dispute Monitoring Program or for other activity that causes undue harm to the Visa system.

ID# 0008667	Edition: Apr 2020	Last Updated: Apr 2020

10.4.9   Issuer Fraud Monitoring

10.4.9.1   Visa Issuer Monitoring Program (VIMP)

In the AP Region,[1] Canada Region, CEMEA Region, Europe Region, LAC Region, US Region: Visa monitors Issuers that generate an excessive level of Fraud Activity through the Visa Issuer Monitoring Program (VIMP) and will identify an Issuer under the VIMP if it meets or exceeds both of the following monthly standard thresholds for Card-Absent Environment Fraud Activity monitoring, for either domestic or international activity:

- USD 500,000 fraud amount

- 1% ratio of fraud-to-sales dollar amount

In the US Region: In addition, Visa will identify an Issuer under 3-D Secure Fraud Activity monitoring, for domestic 3-D Secure fraud only, if it meets or exceeds both of the following monthly standard program thresholds:

- USD 100,000 3-D Secure fraud amount

- 0.75% ratio of 3-D Secure fraud-to-sales dollar amount

Visa may modify or create new monthly VIMP performance levels.

Program monitoring includes all Card-Absent Environment Fraud Activity reported by Issuers to Visa in the preceding calendar month and all Card-Absent Environment Sales Transactions settled with the Issuer in the preceding calendar month.

Visa may require the Issuer to deploy appropriate fraud remediation tools or technologies to address unusual activity in the individual cases identified through the VIMP.

An Issuer will exit the VIMP if it is below the program thresholds for 3 consecutive months.

Visa may impose conditions on an Issuer that knowingly acts to circumvent monitoring.

[1] **Effective 18 April 2020**

ID# 0030598   **Edition: Apr 2020 | Last Updated: Apr 2019**

10.4.9.2   High Total Fraud Loss Monitoring Program – Europe Region

In the Europe Region: Visa identifies the 15 Issuers and 15 Acquirers with the highest levels of fraud, in absolute Transaction value terms, as candidates for formal review.

Once identified, Members will be given at least 3 months' notice of the review and asked to agree a review start date with Visa.

Following a review, Members will receive a report from Visa containing recommendations intended to assist them in improving fraud management.

ID# 0029607   **Edition: Apr 2020 | Last Updated: Oct 2016**

10.4.9.3   Visa Issuer Monitoring Program (VIMP) Timelines

In the AP Region,[1] Canada Region, CEMEA Region, Europe Region, LAC Region, US Region: An Issuer that is identified in the Visa Issuer Monitoring Program (VIMP) must comply with the following:

Table 10-7: VIMP Timeline

Program Status	Issuer Actions
Month 1 – 3	• Review portfolio activity, determine the cause of the excessive Card-Absent Environment Fraud Activity and take actions to mitigate the Fraud Activity
Month 4 – 11 Enforcement Period	• Non-compliance assessments apply • Provide to Visa an action plan to reduce the portfolio's Card Absent Environment Fraud Activity
Month 12 Enforcement Period	• Non-compliance assessments apply • Provide to Visa a final, written summary of the portfolio's performance and Card-Environment Absent Fraud Activity remediation initiatives

Visa reserves the right to withhold Visa Dispute Monitoring Program reimbursements to Issuers identified in the enforcement phase of the VIMP program.

[1] **Effective 18 April 2020**

ID# 0030599	Edition: Apr 2020	Last Updated: Oct 2019

10.4.10   Issuer Fraud Monitoring

10.4.10.1 Issuer Customer Validation Requirement

Effective 18 April 2020 in the AP Region, Canada Region, Europe Region, LAC Region, US Region, and effective 1 July 2020 in the CEMEA Region An Issuer whose Cardholder has 5 or more separate Dispute Category 10 (Fraud) Disputes within a maximum period of 12 months must perform a formal review of the Cardholder account and related Disputes to determine if first-party fraud abuse is occurring.

ID# 0030643	Edition: Apr 2020	Last Updated: Apr 2020

10.5   Brand Protection

10.5.1   Global Brand Protection Program

10.5.1.1 Global Brand Protection Program Data Quality

To enable the valid identification of data for the Global Brand Protection Program, an Acquirer must correctly classify its High-Brand Risk Merchants.

If Visa determines that an Acquirer or its Merchant changed, modified, or altered the Merchant name or Merchant data in any way to circumvent the Global Brand Protection Program, Visa may:

- In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Do any of the following:
  - Assess a non-compliance assessment
  - Require the Acquirer to implement risk reduction measures
  - Prohibit the Acquirer from acquiring High-Brand Risk Merchants for a period of one year or more

ID# 0026335   Edition: Apr 2020 | Last Updated: Apr 2020

10.6   Fraud Reporting

10.6.1   Fraud Reporting Requirements

10.6.1.1   Prepaid Clearinghouse Service (PCS) Participation – US Region

In the US Region: An Issuer of Prepaid Cards must:

- Report information from all approved, pending or declined Prepaid Account enrollments, Load Transactions, reloads, unauthorized Transaction requests, Prepaid Account fraud, Transaction Load fraud, Account level fraud and enrollment fraud
- Ensure that it and its agents report complete and correct information, as specified by Visa
- Authorize Visa to use or transfer the information reported to PCS for any purpose permitted by applicable laws or regulations
- Submit all records in accordance with the *Prepaid Clearinghouse Service (PCS) Product Guide and Reporting Requirements* and the Prepaid Clearinghouse Service (PCS) Message Layout

Issuers of Prepaid Cards or Agents optionally subscribing to use PCS:

- Must execute a PCS Participation Agreement
- Are eligible under applicable law to access PCS for fraud prevention purposes

ID# 0029067   Edition: Apr 2020 | Last Updated: Apr 2020

10.6.1.2   Skimming Counterfeit Fraud Data Collection – Europe Region

In the Europe Region: On fraud advice reports, a Member must identify skimmed counterfeit fraud Transactions with POS Entry Mode code 90.

ID# 0029597   Edition: Apr 2020 | Last Updated: Oct 2016

10.6.1.3   Reporting of Chip Card Capability in Fraud Advice Records – Europe Region

In the Europe Region: An Issuer must provide Chip Card capability details in fraud advice records.

An Issuer that fails to correctly report the Card capability in fraud advice records is subject to penalties, including, but not limited to, withdrawal of the Issuer's right to use all Dispute conditions related to the EMV liability shift, until the problem is corrected.

ID# 0029598   Edition: Apr 2020 | Last Updated: Apr 2018

10.6.1.4   Fraud Activity Reporting Compliance – LAC Region

In the LAC Region: An Issuer must report Fraud Activity and comply with all of the following:

- At least 95% of all fraud must be reported. This includes domestic and international, on-us, debit and credit, and ATM Transactions.
- At least 90% of all reported fraud must be classified correctly.
- No more than 5% of all reported fraud can be classified as fraud type 05 (Miscellaneous).
- In at least 90% of reported fraudulent Transactions, mandatory TCR2 fields must match the corresponding BASE II record fields, except the Excluded Transaction Identifier Reason field.

ID# 0007259   Edition: Apr 2020 | Last Updated: Oct 2014

10.6.1.5   Result of Issuer Non-Compliance – AP Region

In the AP Region: An Issuer identified as non-compliant and that fails to resolve areas of non-compliance within a period agreed between the Member and Visa following an on-site review will not be permitted to dispute a transaction under Dispute category 10 (Fraud).

ID# 0001760   Edition: Apr 2020 | Last Updated: Apr 2018

10.7   Card Recovery

10.7.1   Card Recovery at the Point of Sale

10.7.1.1   Merchant Card Recovery Procedures at the Point of Sale

A Merchant must not complete a Transaction and should attempt to recover a Card[1] by reasonable, peaceful means, for any of the following reasons:

- Account Number appears on a Card Recovery Bulletin

- Acquirer or its Authorizing Processor requests its retention

- **Effective through 16 October 2021** 4 digits printed below the embossed or printed Account Number (if present) do not match the first 4 digits of the embossed or printed Account Number

- Merchant has reasonable grounds to believe that the Card is counterfeit, fraudulent, or stolen

A Merchant must notify its Acquirer that it has recovered a Card and ask for further instructions.

[1]   The requirement to attempt to recover the Card does not apply to Mobile Payment Devices.

ID# 0002350	Edition: Apr 2020	Last Updated: Apr 2020

10.7.2   Return of Recovered Cards

10.7.2.1   Recovered Card Handling and Notification Requirements

A Member must maintain an inventory log of recovered Cards that includes a record of at least all of the following:

- Date of Card recovery (DD/MM/YYYY)

- Location of Card recovery

- First 6 digits and last 4 digits of the Account Number (if present on the Card)

- Cardholder name: Title (if applicable), first letter of first name and first and last letters of last name

- Printed names and signatures of all parties counting, logging, or destroying the Cards

- If the Card was retained by a law enforcement agency, name of agency and contact information

- Date of Card destruction (DD/MM/YYYY)

In the Europe Region: An Acquirer must retain the record in the inventory log for at least 3 months.

The Member or its Agent must comply with all of the following requirements for the secure destruction of recovered Cards:

- Within 5 business days of recovering a valid or counterfeit Card, ensure that the Card is securely destroyed through shredding or incineration

- If the Card cannot be destroyed immediately upon receipt by the secure destruction location, store the Card in a secure environment under dual control until the Card can be properly destroyed.

- Before secure destruction, maintain the Cards as specified in PCI DSS

- Render all images, Account Numbers, and generic identifiers completely unusable or unreadable. Cutting the Card in half and disposing of it in the trash does not comply with this requirement.

- Ensure that all Cards have been destroyed before leaving the destruction area

- If a secure destruction entity is contracted to destroy Cards, ensure that the entity presents a certificate of destruction once the destruction process is completed.

Upon recovery of a valid or counterfeit Visa Card, the Member must send[1] a Notification to the Issuer, through Visa Resolve Online or the Electronic Documentation Transfer Method, that the Card was recovered and destroyed. The Notification must be sent no later than either:

- 5 business days after the Visa Card is recovered

- For a Card recovered at an ATM, 5 business days after the Card is received at the Acquirer's card return center, if applicable

The Notification must include all of the following information:

- Date of Card recovery (DD/MM/YYYY)

- Location of Card recovery

- First 6 digits and last 4 digits of the Account Number (if present on the Card)

- Cardholder name: Title (if applicable), first letter of first name and first and last letters of last name

- If the Card was retained by a law enforcement agency, name of agency and contact information

- If the Acquirer paid an appropriate Card recovery reward to its Merchant, the Fee Collection Transaction amount that will be submitted to the Issuer for reimbursement

- Date of Card destruction (DD/MM/YYYY)

In the Europe Region: The Cardholder Verification Method transmitted in the Clearing Record must be retained by Issuers and included in the Dispute and the fraud information message.

[1] For a Non-Reloadable Prepaid Card recovered without a Pickup Response or a specific request from the Issuer, the

Member must cut the Card and render it unusable but is not required to notify the Issuer that the Card was recovered.

ID# 0008090	Edition: Apr 2020 | Last Updated: Oct 2019

10.7.2.2   Merchant Recovered Card Return Procedures – US Region

In the US Region: A Merchant that recovers a Visa Card must both:

- Cut the Visa Card horizontally so as not to damage the Magnetic Stripe, Chip, hologram (if applicable), and embossed or printed Account Number (if applicable)
- Immediately send it to either:
  - Its Acquirer
  - A VisaNet Interchange Center, if Visa is designated as the Merchant's Authorizing Processor

The requirement to return the Card does not apply to Non-Reloadable Prepaid Cards recovered without a Pickup Response or request from the Issuer.

For a Non-Reloadable Prepaid Card recovered without a Pickup Response or a specific request from the Issuer, the Merchant or Acquirer must cut the Card and render it unusable.

For a Non-Reloadable Prepaid Card where an Issuer Pickup Response has been sent, the Merchant should attempt to recover the Card and:

- Cut the Card horizontally so as not to damage the Magnetic Stripe, Chip, hologram (if applicable), and embossed or printed Account Number (if applicable)
- Immediately send it to either:
  - Its Acquirer
  - A VisaNet Interchange Center, if Visa is designated as the Merchant's Authorizing Processor

If a recovered Visa Card was retained by a law enforcement agency, the Merchant must provide a legible copy of the front and back of the Visa Card to its Acquirer or a VisaNet Interchange Center, as applicable.

ID# 0008092	Edition: Apr 2020 | Last Updated: Apr 2019

10.7.2.3   Acquirer Recovered Card Procedures – Additional Notification Requirement – US Region

Effective through 16 October 2021 In the US Region: An Acquirer must immediately advise either of the following of the recovery of a Card:

- The Issuer, if the Visa Card is recovered because the first 4 digits of the embossed or printed Account Number (if present) do not match the 4 digits printed above or below the Account Number
- Visa, if the embossed or printed BIN is not assigned to a Member

An Acquirer must retain a legible copy of the front and back of the recovered Card.

ID# 0008094	Edition: Apr 2020 | Last Updated: Apr 2020

10.7.3   Recovered Counterfeit Cards

10.7.3.1   Unattended Cardholder-Activated Terminal Card Retention

If an Unattended Cardholder-Activated Terminal has the ability to retain a Card, it may retain a Card only upon the specific request of the Issuer.

If a Card is retained and removed from the terminal by a Merchant, the Merchant must do all of the following:

- Log it under dual custody immediately after removal from the terminal
- Render it unusable
- Send it to its Acquirer

If a Card is retained and removed from the terminal by an Acquirer, the Acquirer must do all of the following:

- Log it under dual custody immediately after removal from the terminal
- Render it unusable following secure Card destruction requirements, as specified in *Section 10.7.2.1, Recovered Card Handling and Notification Requirements*
- Notify the Issuer, through Visa Resolve Online, that the Card was recovered, as specified in *Section 10.7.2.1, Recovered Card Handling and Notification Requirements*

ID# 0004823	Edition: Apr 2020 | Last Updated: Apr 2017

10.7.4   Card Recovery Bulletin (CRB)

10.7.4.1   Card Recovery Bulletin (CRB) Dispute Rights

An Acquirer may be subject to a Dispute for below-Floor Limit Transactions if the Account Number appears on the Card Recovery Bulletin (CRB). Dispute rights begin on the effective date of the CRB in which the Account Number is listed.

ID# 0003981   Edition: Apr 2020 | Last Updated: Apr 2018

10.8   Lost or Stolen Cards

10.8.1   Lost or Stolen Card Reporting

10.8.1.1   Lost/Stolen Card Reporting – Issuer Actions

An Issuer participating in Lost/Stolen Card Reporting must, on behalf of another Issuer, both:

- Accept reports of lost or stolen products from Cardholders or their designated representative
- Notify the Card Issuer

ID# 0008549   Edition: Apr 2020 | Last Updated: Oct 2014

10.8.1.2   Issuer Notification of Lost or Stolen Card

A Member must do all of the following:

- Provide the Issuer with the information required on the lost or stolen Card report
- If an incomplete Account Number is provided, supply the Issuer with the address and telephone number where the Cardholder may be contacted
- Notify Visa Global Customer Care Services if unable to establish contact with the Issuer

ID# 0002183   Edition: Apr 2020 | Last Updated: Apr 2018

10.9   PIN Security Requirements

10.9.1   PIN Requirements

10.9.1.1   Visa PIN Security Program Requirements

An Acquirer and its Merchant or agent that processes PINs for Visa Transactions must comply with the security requirements specified in the PIN Management Requirements Documents and *Visa PIN Security Program Guide.*

ID# 0027086   Edition: Apr 2020 | Last Updated: Oct 2018

10.10   Account Data Compromise

10.10.1   Global Compromised Account Recovery (GCAR) Program

10.10.1.1   Global Compromised Account Recovery (GCAR) Program Qualification – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: An Issuer may recover a portion of its operating expenses associated with an Account Data Compromise Event involving a compromise of either:

- In a Card-Absent Environment, a Chip Card's Account Number and expiration date

- In a Card-Present Environment, a Chip Card's Account Number and Card Verification Value

Visa has the authority and discretion to determine Account Data Compromise Event qualification, Operating Expense Recovery amounts, Issuer eligibility, and Acquirer liability under the GCAR program, in accordance with the *Visa Global Compromised Account Recovery (GCAR) Guide* and the available information regarding each compromise event.

ID# 0026564	Edition: Apr 2020 | Last Updated: Apr 2018

10.10.1.2   Acquirer Safe Harbor for Registered Agents – Europe Region

In the Europe Region: An Acquirer must ensure that its Merchants and Sponsored Merchants use only agents that are registered with Visa and appear on the Visa list of agents that provide payment-related services (including services that operate under contractual obligations to the Merchant or Sponsored Merchant to control access to Cardholder data) to Merchants or Sponsored Merchants, except payment application software providers.

To qualify for safe harbor in the event of an Account Data Compromise Event, the agent must both:

- Be listed with Visa before the date of notification of the suspected or confirmed data compromise

- Demonstrate that it was one or more of the following:

  - Successfully assessed by a qualified security assessor as Payment Card Industry Data Security Standard (PCI DSS)-compliant at the time of the data compromise

  - Self-assessed against the PCI DSS. The PCI Forensic Investigator report must confirm that the agent complied with the security measures specified in the self-assessment questionnaire submitted during the registration process.

– Out of scope of the PCI DSS. The PCI Forensic Investigator report must confirm that the agent did not have access to or control over the Cardholder data that was compromised.

An Acquirer whose Merchant or Sponsored Merchant suffers a data compromise through an agent that complies with these requirements is not subject to non-compliance assessments for compromised Account Information and Transaction Information.

ID# 0029584	Edition: Apr 2020 | Last Updated: Apr 2018

10.11   Terminated Merchants

10.11.1   Retention of Merchant Records

An Acquirer or a Payment Facilitator must keep a complete, well-documented file containing Merchant records, including any information connected to an investigation, for at least 2 years after Merchant Agreement termination.

An Acquirer or a Payment Facilitator of a Merchant or Sponsored Merchant that is undergoing a forensic investigation must also notify Visa when it receives notice or otherwise becomes aware that the Merchant has terminated its Merchant Agreement.

ID# 0008474	Edition: Apr 2020 | Last Updated: Apr 2018

10.11.2   Required Use of Terminated Merchant Database

10.11.2.1   Terminated Merchant Listing on Terminated Merchant Database – Third Party Agent –AP Region and Europe Region

In the AP Region (Australia, Cambodia, Mainland China, Hong Kong, India, Indonesia, Macau, Malaysia, New Zealand, Philippines, Singapore, Sri Lanka, Thailand, Vietnam): An Acquirer must ensure that a terminated Merchant, Sponsored Merchant, or Third Party Agent (including, but not limited to, a Payment Facilitator, Marketplace, Staged Digital Wallet Operator (SDWO), or Independent Sales Organization) is added to the Visa Merchant Screening Service (VMSS) if VMSS listing criteria are met.

In the Europe Region: An Acquirer must ensure that a terminated Merchant, Sponsored Merchant or Third Party Agent (including, but not limited to, a Payment Facilitator, Marketplace, Staged Digital Wallet Operator (SDWO) or Independent Sales Organization) is added to the Visa Merchant Screening Service (VMSS) if VMSS listing criteria are met.

ID# 0026433	Edition: Apr 2020 | Last Updated: Apr 2019

10.11.2.2   Terminated Merchant Information Requirements – AP Region

In the AP Region: The file of terminated Merchants must include at least all of the following:

- Merchant Agreement and addenda

- Deposit history and monitoring reports

- Details on the number, total amount, and reasons for any Disputes received

- All Acquirer/Merchant correspondence

- All Visa Fraud Monitoring Program reports relating to the Merchant

- Names and ID numbers of suspect employees

- Written notification of termination or intent to terminate

- Any other supporting documentation that itemizes the details leading to the decision to terminate the Merchant

ID# 0007371	Edition: Apr 2020 | Last Updated: Apr 2018

10.11.2.3   Common Terminated Merchant Database Requirements – Canada Region

In the Canada Region: An Acquirer must comply with all of the following:

- Use an externally managed common terminated Merchant database

- Concurrent with the closure of a Merchant Outlet, list the Merchant on a common terminated merchant database for a period of 3 years if the Merchant violated the Merchant Agreement and was subsequently terminated for cause

- Retain for 3 years Merchant Agreement termination information

ID# 0007377	Edition: Apr 2020 | Last Updated: Oct 2014

10.11.2.4   Terminated Merchant File Listing Requirements – US Region

In the US Region: An Acquirer must add a terminated Merchant to the Terminated Merchant File no later than close of business on the day following the date the Merchant is notified of the intent to terminate the agreement. An Acquirer must list the Merchant if terminated for one or more of the following reasons:

- The Merchant was convicted of credit or debit card fraud.

- The Merchant deposited excessive Counterfeit Transactions.

- The Merchant deposited excessive Transactions unauthorized by Cardholders.

- The Merchant deposited Transaction Receipts representing sales of goods or services generated by another Merchant (laundering).
- The Acquirer received an excessive number of Disputes due to the Merchant's business practices or procedures.

ID# 0007386   Edition: Apr 2020 | Last Updated: Apr 2018

10.11.2.5   Terminated Merchant File Information Requirements – US Region

In the US Region: An Acquirer must add a Merchant to the Terminated Merchant File within 24 hours of determining that:

- The Merchant was terminated for reasons other than those listed in *Section 10.11.2.4, Terminated Merchant File Listing Requirements – US Region*
- Within 90 calendar days of the termination date, the Acquirer determines that the Merchant should have qualified for the listing

The Merchant listing must include the:

- Business name
- Names and identification of principals of terminated Merchants

The Acquirer must report terminated Merchants, as specified.

ID# 0007969   Edition: Apr 2020 | Last Updated: Oct 2014

10.11.2.6   Terminated Merchant File Compliance – US Region

In the US Region: A Member that fails to comply with the Terminated Merchant File requirements may be subject to Compliance, including liability for losses incurred by another Member as a result of the failure to comply.

ID# 0008174   Edition: Apr 2020 | Last Updated: Oct 2014

10.11.2.7   Deletion from or Correction Request for Terminated Merchant File – US Region

In the US Region: Only the Member that added the Merchant to the Terminated Merchant File may request deletion of the Merchant name or information.

A Member that incorrectly adds a Merchant to the file must request correction of the file immediately upon recognition of an error.

ID# 0007963	Edition: Apr 2020 | Last Updated: Oct 2014

10.12   Visa Risk Products

10.12.1   Address Verification Service (AVS)

10.12.1.1 Address Verification Service (AVS) Results Code Population – Canada Region

In the Canada Region: An Acquirer participating in the Address Verification Service (AVS) must populate the AVS results code received in the BASE I Authorization Response message in a Transaction's corresponding BASE II Clearing Record.

ID# 0028293	Edition: Apr 2020 | Last Updated: Oct 2014

10.12.1.2 Address Verification Service (AVS) Participation – US Region

In the US Region: An Issuer must:

- Participate in the Address Verification Service
- Perform address verification for each Address Verification Service inquiry

ID# 0004679	Edition: Apr 2020 | Last Updated: Oct 2014

10.12.1.3 Address Verification Service (AVS) at Unattended Cardholder-Activated Terminals – US Region

In the US Region: An Automated Fuel Dispenser (AFD) Merchant must perform an Address Verification Service (AVS) inquiry if either:[1]

- The AFD Merchant is located in a high-fraud area, as specified in the *AVS ZIP Requirements for US AFD Merchants in High-Fraud Geographies*
- The AFD Merchant has been identified under the Visa Fraud Monitoring Program

If an Unattended Cardholder-Activated Terminal (UCAT) assigned MCC 4111 (Local and Suburban Commuter Passenger Transportation, Including Ferries), 4112 (Passenger Railways), or 5542 (Automated Fuel Dispensers) requests a Cardholder's postal code and performs an Address Verification Service (AVS) inquiry, it must comply with all of the following:

- Not request any postal information other than the zip code
- Not prompt for any additional information (for example: CVV2)

- Not perform AVS inquiry only for Visa Cards, if the UCAT also accepts other payment brands that support AVS

- Provide attended Transaction capabilities in the immediate vicinity of the UCAT that prompts for AVS information

- Either display an affixed sticker or include electronic on-screen language to direct a non-US Cardholder or any impacted Cardholder of a US Region-issued Prepaid Card to an attendant if the Transaction is declined due to non-support of AVS

- For a UCAT assigned MCC 4111 or 4112, either of the following:

  - Prompt for AVS information only for Transactions on Cards issued in the US Region

  - Not prompt for AVS information for Transactions less than USD 25 on Cards not issued in the US Region

[1] Does not apply to an AFD Merchant that provides services only to its membership base

ID# 0027807	Edition: Apr 2020 | Last Updated: Apr 2020

10.12.1.4   Address Verification Service (AVS) Eligible Transactions

A Merchant may use the Address Verification Service (AVS) for a Transaction either:

- In a Card-Absent Environment

- In the US Region: At an Unattended Cardholder-Activated Terminal assigned one of the following MCCs:

  - 4111 (Local and Suburban Commuter Passenger Transportation, Including Ferries)

  - 4112 (Passenger Railways)

  - 5542 (Automated Fuel Dispensers)

ID# 0029279	Edition: Apr 2020 | Last Updated: Oct 2017

10.12.2   Card Verification Value 2 (CVV2)

10.12.2.1   Card Verification Value 2 (CVV2) Requirements – AP Region (Australia, Hong Kong, New Zealand)

In the AP Region (Australia, Hong Kong, New Zealand): An Electronic Commerce Merchant must capture the Card Verification Value 2 (CVV2) and include it in the Authorization Request.

This does not apply to:

- A Transaction that uses Visa Secure[1]

- A Transaction involving a Visa Commercial Card Virtual Account

- A Transaction conducted through Visa Checkout

- A Transaction initiated with a payment Token

[1] A Merchant must adhere to an Issuer's requested authentication method.

ID# 0026176   **Edition: Apr 2020 | Last Updated: Apr 2019**

10.12.2.2   Card Verification Value 2 (CVV2) Requirements – Canada Region

In the Canada Region: An Acquirer participating in the Card Verification Value 2 (CVV2) service must populate the CVV2 results code received in the Authorization Response in a Transaction's corresponding Clearing Record.

A Mail/Phone Order Merchant or Electronic Commerce Merchant must capture the CVV2 and include it in the Authorization Request.

This does not apply to:

- A Transaction that uses a Stored Credential

- A Transaction initiated with a payment Token

- A Transaction in which a paper order form is used

- A Transaction involving a recurring or installment payment

- A Transaction conducted through a digital wallet such as Visa Checkout

- A Transaction originating from an indirect sales channel

- A delayed charge Transaction

- A "No-Show" Transaction

- A Mail Order Telephone Order (MOTO) transaction where the CVV2 data is captured manually and provided in written form

- A Mass Transit Transaction

- A payment Token provisioning request

- A Transaction involving an Incremental Authorization Request

- A Transaction that received a Decline Response and is resubmitted for Authorization, as specified in *Section 7.3.6.1, Preauthorized Transaction Decline Response*

- A Transaction where the merchant is allowed to submit a new Authorization Request for the same Transaction

- A Merchant Credit Transaction Authorization Request

ID# 0000675	Edition: Apr 2020	Last Updated: Apr 2019

10.12.2.3   Card Verification Value 2 (CVV2) Requirements – Europe Region

In the Europe Region: For Transactions occurring in a Card-Absent Environment:

- A Member must be certified by Visa for Card Verification Value 2 processing for Intraregional Transactions.

- An Issuer that is not certified is considered to not be participating in the CVV2 service and will lose fraud Dispute rights under Dispute Condition 10.4: Other Fraud-Card-Absent Environment.

- The Issuer is liable for an approved Transaction with a CVV2 result code N.

An Acquirer must ensure that the CVV2 is present in all Authorization Requests for Transactions in a Card-Absent Environment, except:

- A delayed charge Transaction

- A No-Show Transaction

- A Transaction in which a paper order form is used

- A Transaction conducted through Visa Checkout

- A Transaction using a Stored Credential

- A mail order Transaction where the CVV2 data is captured manually and provided in written form

- A Mass Transit Transaction

- A payment Token provisioning request

- A Transaction initiated with, or for, a payment Token

- A Transaction involving an Incremental Authorization Request

- A Transaction that received a Decline Response and is resubmitted for Authorization, as specified in *Section 7.3.6.1, Preauthorized Transaction Decline Response*

- A Transaction where the Merchant is allowed to submit a new Authorization Request for the same Transaction

ID# 0029600	Edition: Apr 2020	Last Updated: Apr 2018

10.13   Advanced Authorization

10.13.1   Visa Advanced Authorization

10.13.1.1 Visa Advanced Authorization Participation

To implement Visa Advanced Authorization[1], an Issuer and its processor must comply with the certification requirements for Visa Advanced Authorization.

In the LAC Region: Issuers must implement a risk-scoring real-time fraud prevention tool and/or Visa Advanced Authorization and Visa Risk Manager for all products, except Prepaid Cards.

In the US Region: Visa Advanced Authorization data is provided to all Issuers, and an Issuer is responsible for Visa Advanced Authorization fees, regardless of whether or not the Issuer uses the data.

[1] A real-time risk management tool that delivers risk data to Issuers in the Authorization Request to aid early fraud detection.

ID# 0008446	Edition: Apr 2020 | Last Updated: Apr 2020

10.14   Transaction Alerts

10.14.1   Transaction Alerts Requirements

10.14.1.1 Transaction Alerts Service Participation

If an Issuer participates in the Visa Transaction Alerts Service, the Issuer or the Issuer's agent must do all of the following:

- Register with Visa by submitting a completed *Visa Transaction Alerts Service Participation Agreement*
- Provide to Visa Payment Credentials that are eligible to enroll in the service
- Disclose to participating Cardholders which Transactions will and will not trigger Cardholder notification

In the Europe Region: An Issuer that participates in the Visa Alerts Data Feed Service must register with Visa.

In the Canada Region, LAC Region, US Region: An Issuer must provide its Cardholders the option to participate in a service that delivers Transaction alerts for Transactions processed on a consumer Card, excluding a Non-Reloadable Prepaid Card, and routed as follows:

- Visa Transactions routed through VisaNet

- Plus Transactions routed through the Plus Network

- In the US Region only, Interlink Transactions routed through the Interlink Network

The Issuer may offer this service either itself, through a VisaNet Processor, a third-party service provider, or the Visa Transaction Alerts Service.

ID# 0025735	Edition: Apr 2020 | Last Updated: Apr 2020

10.14.1.2   Visa Alerts Service Participation Requirements – Europe Region

In the Europe Region: An Issuer that participates in a Visa Alerts Service must do all of the following:

- Provide to enrolled Cardholders terms and conditions that include all of the following:

  – Terms regarding the use of personal data, in compliance with applicable laws or regulations, including any required explicit consents

  – The cancellation policy for Visa Alerts

  – The applicable fees for using Visa Alerts

  – Details of how to unsubscribe from Visa Alerts

- Ensure that the Cardholder details communicated to Visa are correct and kept current. This information must be communicated through the Cardholder enrollment and update interface of the Visa Alerts Service.

- Use the Cardholder data collected through the use of the Visa Alerts Service for purposes other than sending Alerts only if explicit consent has been granted by the Cardholder

- Include all of the following in the body of the Alert:

  – As required by applicable laws or regulations, details of how the Cardholder can unsubscribe from Visa Alerts

  – At least one reference to "Visa"

  – At least one of the following data fields:

    ▪ The last 4 digits of the Payment Credential

    ▪ Merchant name

    ▪ Transaction Amount

    ▪ Transaction Currency

    ▪ Transaction Date

- Transaction time
- Balance of the Card account (if provided by the Issuer)

Alerts will not be considered as evidence for dispute resolution.

ID# 0029877	Edition: Apr 2020 | Last Updated: Apr 2020

10.15   National Card Recovery File

10.15.1   National Card Recovery File – US Region

10.15.1.1   National Card Recovery File Card Verification Requirements – US Region

In the US Region: A Member, non-Member Authorizing Processor, and their Merchants must use the National Card Recovery File only as specified in the *Card Recovery Bulletin Service (CRB) User's Guide*.

ID# 0003851	Edition: Apr 2020 | Last Updated: Oct 2016

10.16   Visa Secure

10.16.1   Visa Secure General Participation Requirements

10.16.1.1   Visa Secure Participation Requirements

A Member that participates in Visa Secure must:

- Complete the Visa Secure enrollment process
- If the Member is a Sponsored Member, obtain permission from its Principal-Type Member
- As applicable, implement product security measures
- For 3-D Secure 1.0, ensure that its Visa Secure components have successfully met the requirements of the Visa 3-D Secure Vendor Compliance Testing Program
- For 3-D Secure 2.0, ensure that its Visa Secure components have successfully met the requirements of the EMVCo 3-D Secure 2.0 Compliance Testing Program and Visa's 3-D Secure 2.0 Test Suite
- Only use a Digital Certificate issued by or associated with Visa as an Authentication Mechanism for a Visa product or service

An Issuer must participate in Visa Secure, as follows:

Table 10-8: Country/Territory-Specific Visa Secure Participation Requirements

Country/Territory	Applicable Products
AP Region	
Australia	In both Visa Secure with 3-D Secure 1.0 and Visa Secure with 3-D Secure 2.0: • Credit Cards[1] • Debit Cards[1] • Reloadable Prepaid Cards
Effective 18 April 2020 Cambodia, Hong Kong, Indonesia, Macau, Malaysia, Philippines, Singapore, South Korea, Taiwan,[3] Thailand, Vietnam	In both Visa Secure with 3-D Secure 1.0[2] and Visa Secure with 3-D Secure 2.0: • Credit Cards • Debit Cards
India	• Credit Cards • Debit Cards • Reloadable Prepaid Cards
New Zealand	In both Visa Secure with 3-D Secure 1.0 and Visa Secure with 3-D Secure 2.0: • Credit Cards[1] • Debit Cards[1] • Reloadable Prepaid Cards
Canada Region	
Canada	Visa Debit Category Cards
CEMEA Region	
Nigeria	All Cards
Europe Region	
Europe	**Effective 14 March 2020** in Visa Secure with 3-D Secure 2.1: • Credit Cards • Debit Cards

Table 10-8: Country/Territory-Specific Visa Secure Participation Requirements (continued)

Country/Territory	Applicable Products
	• Visa Commercial Cards • Reloadable Prepaid Cards **Effective 14 September 2020** in Visa Secure with 3-D Secure 2.2: • Credit Cards • Debit Cards • Visa Commercial Cards • Reloadable Prepaid Cards
LAC Region	
Brazil	• Debit Cards • Visa Electron Cards
[1] This does not apply to Virtual Accounts associated with Visa Commercial Cards. [2] Only applies to an Issuer that participates in Visa Secure with 3-D Secure 1.0 before 18 April 2020 [3] **Effective 17 October 2020**	

ID# 0026275   Edition: Apr 2020 | Last Updated: Apr 2020

10.16.2   Visa Secure Issuer Participation Requirements

10.16.2.1   Participant Use of Visa Secure Data – Use and Disclosure of Confidential Consumer Cardholder Information

Confidential Consumer Cardholder Information received in connection with participation in Visa Secure shall not be used for marketing purposes, or disclosed to any third party for such use.

ID# 0030113   Edition: Apr 2020 | Last Updated: Apr 2019

10.16.2.2 Issuer 3-D Secure Security Requirements

An Issuer that does not operate its own access control server (ACS) must both:

- Use either of the following to operate the ACS or directory server (DS):

  – The Visa Consumer Authentication Service

  – An ACS or DS service provider listed on the *Visa Global Registry of Service Providers*

- Immediately notify Visa if the approved ACS or DS service provider is unable to uphold its 3-D Secure Security Program responsibilities

ID# 0029040	Edition: Apr 2020 | Last Updated: Apr 2018

10.16.2.3   Visa Secure Cardholder Enrollment

During Cardholder enrollment in Visa Secure, an Issuer that participates in Visa Secure must use a combination of on-Card and off-Card data.

ID# 0004045	Edition: Apr 2020 | Last Updated: Apr 2019

10.16.2.4   Cardholder Authentication Verification Value (CAVV) Requirements

An Issuer that participates in Visa Secure must:

- Include a Cardholder Authentication Verification Value (CAVV) in Authentication Confirmations and Attempt Responses

- Retain a log of all Authentication Requests and Authentication Records

- Provide the log to Visa at Arbitration or Compliance

- Submit a copy of all Visa Secure Authentication Records

- Verify the CAVV. If the CAVV is not verified during Authorization by the Issuer or by Visa, the CAVV is assumed to be valid.

- **Effective 17 October 2020** In the Canada Region, Europe Region, LAC Region, US Region: Support CAVV version 7 for all Visa Secure with EMV 3-D Secure Transactions

- **Effective 17 April 2021** In the AP Region, CEMEA Region: Support CAVV version 7 for all Visa Secure with EMV 3-D Secure Transactions

- In the US Region: Provide Visa with its CAVV keys for Stand-In Processing

For a 3-D Secure 1.0 Authentication Request, if an Issuer does not support Visa Secure, Visa will respond to an Authentication Request, on behalf of the Issuer, with an Attempt Response that contains a CAVV.

Effective 15 August 2019 for the Canada Region, LAC Region, effective 14 March 2020 for the Europe Region, effective 18 April 2020 for the AP Region, CEMEA Region, and effective 31 August 2020 for the US Region For a 3-D Secure 2.0 Authentication Request, if an Issuer does not

support Visa Secure, Visa will respond to an Authentication Request, on behalf of the Issuer, with an Attempt Response that contains a CAVV.

ID# 0008807	Edition: Apr 2020	Last Updated: Apr 2020

10.16.2.5   Visa Secure Unable-to-Authenticate Response Conditions

An Issuer that responds to an Authentication Request with an Unable-to-Authenticate Response must do so only under one or more of the following conditions:

- The Issuer experiences technical problems that prevent a timely response.
- Authentication data received from the Merchant does not comply with the 3-D Secure Specification.
- The Transaction is attempted with a Non-Reloadable Prepaid Card.

ID# 0006914	Edition: Apr 2020	Last Updated: Apr 2019

10.16.2.6   Visa Secure Issuer Requirements – AP Region (Mainland China)

In the AP Region (Mainland China): An Issuer must ensure that its Visa Secure program provides a dynamic Authentication Mechanism to Cardholders such that the data elements used in one Transaction cannot be reused in another Transaction within a pre-defined time frame.

ID# 0025711	Edition: Apr 2020	Last Updated: Apr 2019

10.16.2.7   Visa Secure Issuer Requirements – AP Region (India)

In the AP Region (India): An Issuer must authorize only a domestic Electronic Commerce Transaction with an Electronic Commerce Indicator 5 (Secure Electronic Commerce Transaction).

ID# 0026539	Edition: Apr 2020	Last Updated: Apr 2019

10.16.2.9   Issuer Use of Visa Secure – Europe Region

In the Europe Region: An Issuer that submits Secure Electronic Commerce Transactions must use Visa Secure.

ID# 0029696	Edition: Apr 2020	Last Updated: Oct 2019

Visa Product and Service Rules

10.16.2.10 Visa-Recognized Payment Authentication Method – Issuer Requirements – Europe Region

In the Europe Region: An Issuer must do all of the following:

- Support a Visa-recognized payment Authentication Method
- Notify its Cardholders of the availability of Visa-recognized payment Authentication Methods
- Provide a Visa-recognized payment Authentication Method to a Cardholder upon Cardholder request
- Monitor Electronic Commerce Transactions

This requirement does not apply to Visa Commercial Cards and Cards bearing the Plus Symbol.

ID# 0029798	**Edition: Apr 2020	Last Updated: Oct 2016**

10.16.3   Visa Secure Acquirer and Merchant Participation Requirements

10.16.3.1   Visa Secure Acquirer and Merchant Participation Requirements

An Acquirer must use Electronic Commerce Indicator 5 or 6 in the Clearing Record only if the Authorization Request included the Cardholder Authentication Verification Value (CAVV) (for ECI 6, if provided by the Issuer or Visa).

ID# 0004616	**Edition: Apr 2020	Last Updated: Apr 2019**

10.16.3.2   Electronic Commerce Authentication Data Prohibitions – US Region

In the US Region: In an Authorization Request, an Electronic Commerce Merchant must not transmit Authentication Data specific to one Transaction with another Transaction, except when either:

- Two Transactions are related due to a partial Advance Payment.
- All items of an order cannot be shipped at the same time.

ID# 0004636	**Edition: Apr 2020	Last Updated: Apr 2020**

10.16.3.3   Electronic Commerce Indicator Requirement for High-Risk Merchants – US Region

In the US Region: An Acquirer must ensure that its Merchant that participates in Visa Secure transmits an Electronic Commerce Indicator 7 (Non-Authenticated Security Transaction) in the

Authorization Request and Clearing Record for fully authenticated Transactions and attempted authentication Transactions within 30 days of Notification from Visa that the Merchant is identified in the Visa Fraud Monitoring Program.

This condition also applies if the Merchant enables Visa Secure while identified in the Visa Fraud Monitoring Program.

ID# 0004611	Edition: Apr 2020 | Last Updated: Apr 2019

10.16.4   Use of Visa Authentication Technology

10.16.4.1 Visa Secure Authentication Technology Use

Visa Secure authentication technology must be used solely for the purpose of facilitating a Visa Transaction or Visa Electron Transaction, as applicable. Any other use requires the prior written permission of Visa.

Visa Secure authentication technology includes, but is not limited to, the following:

- Visa Directory Server
- Visa Attempts Access Control Server (AACS)
- Digital Certificates issued or signed by Visa Secure Certificate Authority
- Visa Secure Cardholder Authentication Verification Value (CAVV)

ID# 0029539	Edition: Apr 2020 | Last Updated: Oct 2019

10.17   Credit Bureau Reporting

10.17.1   Credit Bureau Reporting – US Region

10.17.1.1 Credit Bureau Reporting Requirements – US Region

In the US Region: An Issuer must report all Visa Consumer Credit Card accounts to at least one credit reporting bureau and comply with the reporting requirements.

An Issuer must report primary Cardholder data through electronic transmission to a credit bureau by billing cycle, within 2 business days of the billing cycle end date.

An Issuer must report primary Cardholder payment information to a credit bureau using B2 Segment data, unless it is already reporting B3 Segment data.

An Issuer must report data for its primary Cardholders in the following fields of the Associated Credit Bureaus Metro format:

- Full first name, last name, and middle initial

- Generation code (abbreviations such as "Jr.," "Sr.," "II," "III")

- Social Security number

- Valid and complete address

- Valid and complete city, state, and ZIP code

- Date of birth

ID# 0003223	Edition: Apr 2020 | Last Updated: Oct 2014

10.17.1.2   Delinquent Account Reporting – US Region

In the US Region: An Issuer must report to a credit bureau as delinquent an account that is 2 payments past due (30 days delinquent).

An Issuer must use the Metro ratings in the standard format specified. If the delinquency progresses, the Issuer must use the standard Metro status code format until the account is charged off, at which time the Issuer must reflect the appropriate charge-off code.

ID# 0003224	Edition: Apr 2020 | Last Updated: Oct 2014

10.17.1.3   Designated Agent for Credit Bureau Interface – US Region

In the US Region: An Issuer designates Visa, Integrated Solutions Concepts, Inc., or their designee to act on the Issuer's behalf as an agent of the Issuer to do all of the following:

- Establish credit bureau reporting standards

- Monitor credit bureau data

- Contract with credit bureaus to receive data and reports for both:

  - Monitoring their handling of Issuer data

  - Comparing that data to Visa-specified credit bureau reporting standards

ID# 0001900	Edition: Apr 2020 | Last Updated: Oct 2014

10.20   Visa Merchant Screening Service

10.20.1   Visa Merchant Screening Service – AP Region and Europe Region

10.20.1.1 Acquirer Participation in the Visa Merchant Screening Service – AP Region and Europe Region

In the AP Region (Australia, Cambodia, Mainland China, Hong Kong, India, Indonesia, Macau, Malaysia, New Zealand, Philippines, Singapore, Sri Lanka, Thailand, Vietnam): An Acquirer must participate in the Visa Merchant Screening Service (VMSS), unless prohibited by applicable laws and regulations.

In the Europe Region: An Acquirer must participate in the Visa Merchant Screening Service (VMSS), unless prohibited by applicable laws and regulations.

The Acquirer must do all of the following:

- Before signing a Merchant Agreement, request information about the Merchant through the VMSS. The Acquirer must not refuse to enter into a Merchant Agreement based solely on information held on the VMSS

- At the beginning of the Acquirer's relationship with the Merchant, notify the Merchant in writing that if the Merchant Agreement is terminated for cause by Visa or the Acquirer, then the Merchant may be listed on the VMSS

- Notify the Merchant in writing if either or both:

  – The Acquirer terminates the Merchant Agreement.

  – The Acquirer has listed the Merchant in the VMSS. The Acquirer must inform the Merchant of its rights under applicable data protection legislation, including subject right of access.

- List complete information for each Merchant terminated for cause on the VMSS by the end of the business day following the day that written notification was sent to the Merchant

- Retain Merchant Agreement termination information as listed on the VMSS

- Provide assistance to an enquiring Member as to the reasons for listing the Merchant

- Pay all associated fees

- In the Europe Region (Estonia): List fraudulent Merchants on the National Merchant Alert List

Visa may impose a non-compliance assessment each time that an Acquirer fails to list a Merchant or Third Party Agent on the VMSS if the entity was terminated for cause.

ID# 0030572   **Edition: Apr 2020 | Last Updated: Apr 2019**

10.20.1.2 Visa Merchant Screening Service – Data Protection Requirements – Europe Region

In the Europe Region: Visa and each Acquirer shall each comply with their respective obligations in relation to applicable data protection legislation as specified in the Guidelines for Terminated Merchant Databases insofar as these apply to the Visa Merchant Screening Service (VMSS). It will provide individuals with rights of access to their personal data where this is requested. Where an individual requests information from Visa regarding what information is stored on the VMSS database in relation to them, Visa will provide a subject right of access form to be completed. Visa will provide the individual concerned with a clear description of the information that is held on the database in relation to that individual upon receipt of the completed form.

Visa provides the VMSS and will ensure that it complies with those requirements of the Guidelines for Terminated Merchant Databases (approved by the Article 29 – Data Protection Working Party) that are allocated to the database operator, as may be amended from time to time.

Visa will comply fully with all applicable European data protection laws in regards to the Personal Data that it processes in the context of the Visa Merchant Screening Service (VMSS) by both:

- Removing Personal Data about a Merchant from the VMSS file if the Merchant's inclusion was not in accordance with VMSS requirements
- Notifying any parties that have accessed the information on that Merchant within the previous 12-month period of the removal

ID# 0030573	Edition: Apr 2020 | Last Updated: Apr 2019

10.20.1.3 Visa Merchant Screening Service Non-Compliance Assessments – Europe Region

In the Europe Region: An Acquirer that does not list its Merchants or applicable Third-Party Agents as required on the Visa Merchant Screening Service (VMSS) may be subject to a non-compliance assessment of EUR 5,000 for each violation, with no monthly maximum.

ID# 0030574	Edition: Apr 2020 | Last Updated: Oct 2018

10.21 Fraud Detection Systems

10.21.1 Fraud Detection Systems – Europe Region

10.21.1.1 Issuer Requirements Relating to Fraud Detection Systems – Europe Region

In the Europe Region: An Issuer must subscribe to and actively participate in one of the following:

- A fraud detection system provided by Visa

- An equivalent authorization scoring neural network or rules-based system approved by Visa

An Issuer that does not comply may be subject to a non-compliance assessment.

ID# 0029605	Edition: Apr 2020	Last Updated: Oct 2016

10.22   Prepaid

10.22.1   Agent Use/Risk Controls

10.22.1.1 Prepaid Card – Use of Agents

A Prepaid Card Issuer that uses a Third Party Agent for its Prepaid Card program must comply with the requirements specified in *Section 10.2, Agents and Processors, Section 10.3, Account and Transaction Information Security,* and Third Party Agent Due Diligence Risk Standards.

ID# 0008356	Edition: Apr 2020	Last Updated: Apr 2020

10.22.1.2 Prepaid Card Issuer Risk Program Requirements

A Prepaid Card Issuer must comply with, and ensure that its applicable Agent complies with, the *Visa Prepaid Issuer Risk Program Standards Guide* and cooperate with Visa, or an entity approved by Visa, for the completion of a periodic review of the Issuer's or its Agent's operations at any time. The Issuer is responsible for the cost of the periodic review.

The Issuer must both:

- Complete the *Prepaid Issuer Self-Assessment Questionnaire* upon entry into the Prepaid Card program and, at minimum, on an annual basis

- Provide to Visa upon request:

  – A copy of the completed *Prepaid Issuer Self-Assessment Questionnaire*

  – A copy of the review report

ID# 0008359	Edition: Apr 2020	Last Updated: Apr 2020

11   Dispute Resolution

11.1   Responsibilities for Dispute Resolution

11.1.1   Mutual Assistance Between Members

A Member must attempt to offer mutual assistance to other Members to resolve disputes between both:

- Its Cardholder and another Member's Merchant
- Its Merchant and another Member's Cardholder

If a Cardholder or Merchant accepts financial liability for a Transaction, its Member must reimburse the other Member directly.

ID# 0030207	Edition: Apr 2020 | Last Updated: Apr 2018

11.1.2   Issuer Responsibilities to Cardholders for Dispute Resolution

An Issuer must resolve Cardholder disputes under the Visa Rules by extending to Cardholders all protections provided on any Visa Card under applicable laws or regulations and by utilizing the Issuer's customary practices to resolve Cardholder disputes, regardless of which type of Visa Card was used.[1] Thus, the resolution of such Cardholder disputes will be the same in similar circumstances regardless of which type of Visa Card was used. The foregoing applies only with respect to Transactions on Cards using the Visa Brand Mark, not to Transactions using any other payment card brand even if such brand is on the Visa Card.

[1] An Issuer must establish enhanced customer support practices to service Visa Signature, Visa Signature Preferred, and Visa Infinite Cardholders during the dispute resolution process.

ID# 0030208	Edition: Apr 2020 | Last Updated: Apr 2018

11.1.3   Visa Right to Grant Exceptions to Dispute Processing Requirements

If a Member misses a deadline or does not submit documentation electronically because of Visa back office service platform failure, Visa may negate the impact by granting an exception to Visa dispute processing deadlines or documentation requirements.

A Member must submit its inquiry to Visa within 15 calendar days from the date of the Visa back office service platform failure.

ID# 0030209	Edition: Apr 2020 | Last Updated: Apr 2019

11.2   Dispute Resolution General Requirements

11.2.1   Dispute Resolution Process General Requirements

For the purpose of calculating a dispute-related timeframe or time limit, the Processing Date of the preceding event (Transaction, Dispute, Dispute Response, pre-Arbitration attempt, Arbitration, or Compliance) is not counted as one day.

The Issuer must not initiate a Dispute for the same Transaction more than once, except for a Dispute initiated under Dispute condition 10.5 (Visa Fraud Monitoring Program).

An Acquirer must not do either of the following:

- Process a Transaction as a first Presentment if the Issuer has previously submitted a Dispute for the same Transaction

- Respond more than once to the original Dispute

If a Member does not respond through Visa Resolve Online (VROL) within the specified timeframe for an action, or accepts responsibility for the Dispute, the Dispute cycle will be considered closed and that Member will be responsible for last amount received by the opposing Member.

The responsible Member must credit the opposing Member on the same processing date of the acceptance through VROL, when required. If the responsible Member does not credit the opposing Member within the specified time limit, Visa will initiate the applicable credit and debit.

A Member must not submit a Fee Collection Transaction for an acceptance of a Dispute.

| ID# 0030211 | Edition: Apr 2020 | Last Updated: Apr 2018 |

11.2.2   Dispute Resolution Process – Dispute Category 10 (Fraud) and 11 (Authorization)

A Member must comply with the following table to process Disputes under Dispute category 10 (Fraud) and Dispute category 11 (Authorization) and related activity.

Table 11-1: Dispute Resolution Process Steps – Category 10 (Fraud) and Category 11 (Authorization)

Dispute Process Stage	Description
Dispute Time limit: See Dispute condition	After receiving a Presentment, an Issuer may initiate a Dispute under the conditions specified for the applicable Dispute category.
Pre-Arbitration Attempt	In response to a Dispute, the Acquirer may make a pre-Arbitration attempt

Table 11-1: Dispute Resolution Process Steps – Category 10 (Fraud) and Category 11 (Authorization) (continued)

Dispute Process Stage	Description
Time limit: 30 calendar days from the Dispute Processing Date[1,2]	as specified under the applicable Dispute condition.

Pre-Arbitration Response
 	
Time limit:
 	
30 calendar days from the Processing Date of the pre-Arbitration attempt
	An Issuer may respond to the pre-Arbitration attempt as follows:
	
	• The Issuer may accept financial responsibility.
	
	• The Issuer may decline the pre-Arbitration attempt if either:
	
	  – The Acquirer provided either:
	
	    ▪ Compelling Evidence
	
	    ▪ Evidence that the Cardholder no longer disputes the Transaction
	
	  – The Issuer provides new documentation or information about the Dispute.
	
	If a full credit was issued and the Cardholder has suffered a loss due to exchange rate differences, the Issuer must only pursue the difference between the credit and debit.
	
	If the Acquirer has supplied Compelling Evidence with its pre-Arbitration attempt, the Issuer must do one of the following:
	
	• In the Europe Region: Both:
	
	  – Contact the Cardholder to review the Compelling Evidence
	
	  – Provide information detailing how the Compelling Evidence has been addressed by the Cardholder and why the Cardholder continues to dispute the Transaction
	
	• For all other Transactions, both:
	
	  – Certify that it has contacted the Cardholder to review the Compelling Evidence
	
	  – Provide an explanation of why the Cardholder continues to dispute the Transaction
	
	• **Effective through 17 April 2020** For Transactions not involving a Member in the Europe Region, for a Dispute under Dispute Condition 10.4: Other Fraud – Card-Absent Environment, either:

Table 11-1: Dispute Resolution Process Steps – Category 10 (Fraud) and Category 11 (Authorization) (continued)

Dispute Process Stage	Description
	– Certify that the name and address supplied does not match the Cardholder name and address – Certify that it has contacted the Cardholder to review the Compelling Evidence, and provide an explanation of why the Cardholder continues to dispute the Transaction • **Effective 18 April 2020** For Transactions not involving a Member in the Europe Region, for a Dispute under Dispute Category 10: Fraud, either: – Certify that the name and address supplied does not match the Cardholder name and address – Certify that it has contacted the Cardholder to review the Compelling Evidence, and provide an explanation of why the Cardholder continues to dispute the Transaction
Arbitration Time limit: 10 calendar days[3] from the Processing Date of the pre-Arbitration response	The Acquirer may file for Arbitration when either: • The Dispute and Pre-Arbitration cycle has been completed and the Member has not been able to resolve the Dispute. • The opposing Issuer has not met the requirements specified in the Visa Rules.
[1] In the CEMEA Region (Nigeria): For a domestic POS Transaction, 5 business days. For a domestic ATM Transaction, 3 business days. [2] In the Europe Region (Poland): For a domestic ATM Transaction, 20 calendar days [3] Plus 30 calendar days for a Group Member	

11.2.3   Dispute Resolution Process – Dispute Category 12 (Processing Errors) and 13 (Consumer Disputes)

A Member must comply with the following table for processing Disputes under Dispute category 12 (Processing Errors) and Dispute category 13 (Consumer Disputes) and related activity.

Table 11-2: Dispute Resolution Process Steps – Category 12 (Processing Errors) and Category 13 (Consumer Disputes)

Dispute Process Stage	Description
Dispute Time limit: See Dispute condition	After receiving a Presentment, an Issuer may initiate a Dispute under the conditions specified for the applicable Dispute category.
Dispute Response Time limit: 30 calendar days from the Dispute Processing Date[1,2,3,4]	The Acquirer may initiate a Dispute Response as specified under the applicable Dispute condition.

Pre-Arbitration Attempt
 	
Time limit:
 	
30 calendar days from the Dispute Response Processing Date
	After receipt of a Dispute Response, the Issuer may make a pre-Arbitration attempt for any of the following reasons:
	
	• The Issuer can provide new documentation or information to the Acquirer about the Dispute.
	
	• If the Acquirer has supplied Compelling Evidence, the Issuer certifies that it has contacted the Cardholder to review the Compelling Evidence and either:
	
	   – In the Europe Region: Can provide information detailing how the Compelling Evidence has been addressed by the Cardholder and why the Cardholder continues to dispute the Transaction
	
	   – For all other Transactions, can provide an explanation of why the Cardholder continues to dispute the Transaction.
	
	• The Issuer changes the Dispute condition after receiving the Dispute Response.
	
	• If the Acquirer provided evidence that the Cardholder no longer disputes the Transaction, the Issuer certifies that the Cardholder still disputes the Transaction.
	
	If a full credit was issued and the Cardholder has suffered a loss due to exchange rate differences, the Issuer must only pursue the difference between the credit and debit.

Pre-Arbitration Response Time limit:	An Acquirer may respond to the pre-Arbitration attempt as follows: • The Acquirer may accept financial responsibility.

Table 11-2: Dispute Resolution Process Steps – Category 12 (Processing Errors) and Category 13 (Consumer Disputes) (continued)

Dispute Process Stage	Description
30 calendar days from the Processing Date of the pre-Arbitration Attempt	• The Acquirer may decline the pre-Arbitration attempt.
Arbitration Time limit: 10 calendar days[5] from the Processing Date of the pre-Arbitration response	The Issuer may file for Arbitration when one of the following occurs: • The Dispute and Pre-Arbitration cycle has been completed and the Issuer has not been able to resolve the dispute. • The Acquirer has not met the requirements specified in the Visa Rules.

[1] In the CEMEA Region (Egypt): For a domestic ATM Transaction, for Dispute conditions 12.6 (Duplication/Paid by Other Means) and 13.9 (Non-Receipt of Cash or Load Transaction Value), 10 calendar days

[2] In the AP Region (India): For a domestic ATM Transaction for Dispute conditions 12.6 (Duplication/Paid by Other Means) and 13.9 (Non-Receipt of Cash or Load Transaction Value), 6 calendar days

[3] In the CEMEA Region (Nigeria): For a domestic POS Transaction, 5 business days. For a domestic ATM Transaction, 3 business days.

[4] In the Europe Region (Poland): For a domestic ATM Transaction, for Dispute conditions 12.6 (Duplication/Paid by Other Means) and 13.9 (Non-Receipt of Cash or Load Transaction Value), 20 calendar days

[5] Plus 30 calendar days for a Group Member

ID# 0030213   **Edition: Apr 2020 | Last Updated: Apr 2019**

11.3   Use of Visa Systems

11.3.1   Use of Visa Systems for Dispute Processing

A Member must use VisaNet or Visa Resolve Online (VROL) to process a financial message arising from a dispute (either Dispute, Dispute Response, pre-Arbitration, or pre-Arbitration response) that has been accepted by VROL.[1,2] This requirement does not apply to domestic Interchange processed under a Private Agreement.

A Member must use VROL[1] to do all of the following:

• Process a Dispute or Dispute Response

• Respond to a Retrieval Request[2]

- Send Dispute-related documentation

- Make a pre-Arbitration or pre-Compliance attempt

- Process a pre-Arbitration or pre-Compliance response

- File an Arbitration or Compliance case[3]

- Withdraw an Arbitration or Compliance case

- File an appeal of an Arbitration or a Compliance decision

VROL questions must be answered in English and any dispute-related documentation must be provided in English, or accompanied by an English translation.

[1] In the Europe Region: This rule does not apply to a Member that chooses a Visa Scheme Processor that is not Visa. Where a Member chooses a Visa Scheme Processor that is not Visa but would like to use Visa for Arbitration and Compliance services, it must send all applicable information to Visa in an electronic format.

[2] A Response to Retrieval Request reason code 27 (Healthcare Auto-substantiation Request) must not be processed using Visa Resolve Online.

[3] A Member must not combine more than 10 disputed Transactions in the same case. The Payment Credential, Acquirer, Merchant Name, Merchant Location, and Dispute condition must be the same in each Dispute.

ID# 0030214	Edition: Apr 2020 | Last Updated: Apr 2020

11.3.2   Transaction Processing Requirements

A Member must process financial messages related to Disputes as follows:

Table 11-3: Financial Message Types – Category 10 (Fraud) and Category 11 (Authorization)

Dispute Process Stage	Transaction Type
Dispute	The Issuer must process a Dispute Financial for the Dispute amount.
Pre-arbitration Acceptance	The Issuer must process a Dispute Financial Reversal on the same Processing Date as the Pre-arbitration acceptance.

Table 11-4: Financial Message Types – Category 12 (Processing Errors) and Category 13 (Consumer Disputes)

Dispute Process Stage	Transaction Type
Dispute	The Issuer must process a Dispute Financial for the Dispute amount.
Dispute Response	The Acquirer must process a Dispute Financial Response.
Pre-arbitration Acceptance	The Acquirer must process a Dispute Financial Response Reversal.

11.3.3   Reversal of a Dispute

If the opposing Member has not already moved to the next stage of the Dispute cycle and neither Member has accepted financial liability, a Member may reverse an action (a Dispute, a Dispute Response, a pre-Arbitration attempt, or a response to a pre-Arbitration attempt) no later than 3[1,2] calendar days after the Processing Date of that action.

[1] One calendar day for a Dispute involving an Original Credit Transaction

[2] This rule does not apply if the Cardholder has contacted the Issuer to confirm that they no longer dispute the Transaction

11.4   Dispute Amount

11.4.1   Dispute and Dispute Response Amount General Requirements

The Dispute amount (specified in the Billing Currency[1]) must be either:

- Actual billed amount
- Partial Transaction amount equal to the disputed amount

The Dispute amount must not exceed the Transaction amount except for Dispute condition 12.2 (Incorrect Transaction Code) where a debit was processed as a credit or a credit was processed as a debit.

If the Dispute is for a partial amount, any surcharge amount must be pro-rated.

The amount contained in a Dispute Response or a pre-Arbitration attempt made by an Acquirer must contain one of the following:

- The same amount in the same Transaction Currency as in the original Presentment
- A partial amount to remedy the Dispute
- The same or corrected amount in the Settlement Currency as received by the Acquirer for the Dispute

[1] In the LAC Region (Venezuela): For an International Transaction, must be in either the Transaction Currency or the Issuer's Settlement Currency

---

11.4.2   Currency Conversion Difference

The party that is assigned or accepts final liability for a Dispute is responsible for the difference between the original Transaction amount and the final Dispute amount that may be caused by currency conversion.

11.4.3   Minimum Dispute Amounts

Minimum Dispute amounts apply as follows:

Table 11-5: Minimum Dispute Amount

Transaction Type	Applicable Dispute Condition	Minimum Dispute Amount	Country/Region
T&E	All except the following Dispute conditions: • 10.1 (EMV Liability Shift Counterfeit Fraud) • 10.5 (Visa Fraud Monitoring Program) • 13.8 (Original Credit Transaction) • 13.9 (Non-Receipt of Cash or Load Transaction Value)	USD 25[1] (or local currency equivalent)	All
Automated Fuel Dispenser	10.3 (Other Fraud – Card-Present Environment)	USD 10 (or local currency equivalent)	All
[1] In the LAC Region (Brazil): This does not apply to a domestic Installment Transaction.			

11.5   Dispute Rights and Restrictions

11.5.1   Prohibition of Multiple Transactions in a Dispute

An Issuer must dispute each Transaction separately.

ID# 0030220	Edition: Apr 2020 | Last Updated: Apr 2018

11.5.2   Use of Compelling Evidence

An Acquirer may submit Compelling Evidence with a Dispute Response or pre-Arbitration attempt, as follows:

Table 11-6: Allowable Compelling Evidence

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
1	Evidence, such as photographs or emails, to prove a link between the person receiving the merchandise or services and the Cardholder, or to prove that the Cardholder disputing the Transaction is in possession of the merchandise and/or is using the merchandise or services.			X	X
2	For a Card-Absent Environment Transaction in which the merchandise is collected from the Merchant location, any of the following: • Cardholder signature on the pick-up form • Copy of identification presented by the Cardholder[2] • Details of identification presented by the Cardholder			X	X
3	For a Card-Absent Environment Transaction in which the			X	X

Table 11-6: Allowable Compelling Evidence (continued)

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
	merchandise is delivered, evidence that the item was delivered to the same physical address for which the Merchant received an AVS match of Y or M. A signature is not required as evidence of delivery.				
4	For an Electronic Commerce Transaction representing the sale of digital goods downloaded from a Merchant's website or application, description of the merchandise or services successfully downloaded, the date and time such merchandise or services were downloaded, and 2 or more of the following: • Purchaser's IP address and the device geographical location at the date and time of the Transaction • Device ID number and name of device (if available) • Purchaser's name and email address linked to the customer profile held by the Merchant • Evidence that the profile set up by the purchaser on the Merchant's website or application was accessed by			X	X

Table 11-6: Allowable Compelling Evidence (continued)

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
	the purchaser and has been successfully verified by the Merchant before the Transaction Date • Evidence that the Merchant's website or application was accessed by the Cardholder for merchandise or services on or after the Transaction Date • Evidence that the same device and Card used in the disputed Transaction were used in any previous Transaction that was not disputed				
5	For a Transaction in which merchandise was delivered to a business address, evidence that the merchandise was delivered and that, at the time of delivery, the Cardholder was working for the company at that address. A signature is not required as evidence of delivery.			X	X
6	For a Mail/Phone Order Transaction, a signed order form			X	
7	For a passenger transport Transaction, evidence that the services were provided and any of the following:			X	X

Table 11-6: Allowable Compelling Evidence (continued)

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
	• Evidence that the ticket was received at the Cardholder's billing address • Evidence that the ticket or boarding pass was scanned at the gate • Details of frequent flyer miles relating to the disputed Transaction that were earned or redeemed, including address and telephone number, that establish a link to the Cardholder • Evidence of any of the following additional Transactions related to the original Transaction: purchase of seat upgrades, payment for extra baggage, or purchases made on board the passenger transport				
8	For Transactions involving a Europe Member, for an Airline Transaction, evidence showing that the name is included in the manifest for the departed flight and matches the name provided on the purchased itinerary			X	
9	For a T&E Transaction, evidence that the services were provided and either:			X	X

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-6: Allowable Compelling Evidence (continued)

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
	• Details of loyalty program rewards earned and/or redeemed including address and telephone number that establish a link to the Cardholder • Evidence that an additional Transaction or Transactions related to the original Transaction, such as the purchase of T&E service upgrades or subsequent purchases made throughout the T&E service period, were not disputed				
10	For a virtual Card Transaction at a Lodging Merchant, evidence of the Issuer's payment instruction sent through Visa Payables Automation, containing all of the following: • Issuer statement confirming approved use of the Card at the Lodging Merchant • Payment Credential • Guest name • Name of the company (requestor) and either their phone number, fax number, or email address			X	

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-6: Allowable Compelling Evidence (continued)

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
11	For a Card-Absent Environment Transaction, evidence that the Transaction used an IP address, email address, physical address, and telephone number that had been used in a previous, undisputed Transaction			X	
12	Evidence that the Transaction was completed by a member of the Cardholder's household or family			X	
13	Evidence that the person who signed for the merchandise was authorized to sign for the Cardholder or is known by the Cardholder				X
14	Evidence of one or more non-disputed payments for the same merchandise or service			X	
15	For a Recurring Transaction, evidence of all of the following: • A legally binding contract held between the Merchant and the Cardholder • The Cardholder is using the merchandise or services • A previous Transaction that was not disputed			X	

Table 11-6: Allowable Compelling Evidence (continued)

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
16	In the Europe Region: Evidence that the Cardholder has been compensated for the value of the merchandise or services through another method				X
17	In the Europe Region: Evidence that the initial Transaction to set up a wallet was completed using Visa Secure but any subsequent Transaction from the wallet that was not completed using Visa Secure contained all wallet-related Transaction data.			X	
18	**Effective for pre-Arbitration attempts processed on or after 18 April 2020** For a US Domestic Card-Present Environment Transaction that is key-entered and did not take place at a Chip-Reading Device, either: • Evidence that the same Card used in the disputed Transaction was used in any previous or subsequent Transaction that was not disputed • Copy of identification presented by the Cardholder,[2] and a signed copy of at least	X	X		

Table 11-6: Allowable Compelling Evidence (continued)

Item #	Allowable Compelling Evidence[1]	Applicable Dispute Condition		Applicable Dispute Condition	
		10.1 (EMV Liability Shift Counterfeit Fraud)	10.3 (Other Fraud – Card-Present Environment)	10.4 (Other Fraud – Card-Absent Environment)	13.1 Merchandise/ Services Not Received
	one of the following: – The receipt – The contract – Invoice that links to the identification presented by the Cardholder				

[1] In the Europe Region: An Acquirer may present Compelling Evidence not listed in this table.

[2] A Merchant must not require positive identification as a condition of Card acceptance, unless it is required or permitted elsewhere in the Visa Rules.

ID# 0030221   **Edition: Apr 2020 | Last Updated: Apr 2020**

11.6   Dispute Categories and Conditions

11.6.1   Dispute Categories Table Format

The Dispute categories and conditions are organized in tables to show the applicable Dispute condition and geographical scope for different rules.

The tables consist of one or 2 columns. The first column typically shows the rule language. The second column, if present, specifies the country or region for which the rule is applicable and uses the following labels:

Table 11-7: Dispute Country/Region Descriptions

Country/Region Label	Description
All	The rule applies to a Transaction between Members anywhere in the world.

Table 11-7: Dispute Country/Region Descriptions (continued)

Country/Region Label	Description
All excluding Europe	The rule applies only to a Transaction that does not involve a Europe Member.
Europe and Interregional including Europe	The rule applies to both: • A Transaction in the Europe Region • An Interregional Transaction between a Member outside the Europe Region and a Member in the Europe Region.
[Region names] Interregional	The rule applies only to an Interregional Transaction between the named Visa Regions (for example: a rule labeled as "Canada/US Interregional" applies only to an Interregional Transaction between the Canada Region and the US Region).
[Region name]	The rule applies only to a Transaction within the named Visa Region (for example: a rule labeled as "AP" applies only to an Intraregional Transaction or Domestic Transaction in the AP Region).
[Country name] Domestic	The rule applies only to a Domestic Transaction within the named country (for example: a rule labeled as "Brazil Domestic" applies only to a Domestic Transaction in Brazil).

ID# 0030222   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.7   Dispute Category 10: Fraud

11.7.1   Dispute Category 10: Cardholder Letter or Certification Requirements

If the Dispute requires an Issuer to provide certification on behalf of the Cardholder, they may only certify if they obtained the dispute information through a secure method, for example:

- Secure online banking: Any method used by the Cardholder that establishes their unique identity through use of a password and/or other login identification method is considered a valid representation of the Cardholder signature
- Secure telephone banking: Where the Cardholder was identified using the same level of security needed to complete a transfer of funds to another financial institution

Instead of an Issuer certification, an Issuer may support the Dispute with a Cardholder[1] letter denying authorization of or participation in a Transaction. If provided to support the Dispute, the letter must be signed by the Cardholder[1] and include all of the following:

- Cardholder's[1] complete or partial Payment Credential

- Merchant name(s)

- Transaction amount(s)

[1] Or Virtual Account holder

ID# 0030223	Edition: Apr 2020 | Last Updated: Apr 2020

11.7.2   Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud

11.7.2.1   Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud for the following reason:

Table 11-8: Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Reasons

Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud Dispute Reasons	Country/Region

The Transaction qualifies for the EMV liability shift, as specified in *Section 1.11.1.2, EMV Liability Shift Participation*, and all of the following:
 	
- The Transaction was completed with a Counterfeit Card in a Card-Present Environment.
- The Cardholder denies authorization of or participation in the Transaction.
- The Card is a Chip Card.
- Either:
  – The Transaction did not take place at a Chip-Reading Device (terminal entry capability code was not 5).
  – The Transaction was Chip-initiated and, if the Transaction was authorized Online, the Acquirer did not transmit the Full-Chip Data to Visa in the Authorization Request.
	All

ID# 0030233	Edition: Apr 2020 | Last Updated: Apr 2018

11.7.2.2   Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Rights

Table 11-9: Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Rights

Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud Dispute Rights	Country/Region
Before initiating a Dispute, an Issuer must report the Fraud Activity to Visa using fraud type code 4.	**All**

ID# 0030234	Edition: Apr 2020 | Last Updated: Apr 2018

11.7.2.3   Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Invalid Disputes

A Dispute is invalid under Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud for any of the following:

Table 11-10: Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Invalid Disputes

Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud Invalid Disputes	Country/Region
- A Chip-initiated Transaction - An Emergency Cash Disbursement - A Fallback Transaction. - A Mobile Push Payment Transaction - A Transaction for which the Authorization record contains POS Entry Mode code 90 and the Service Code encoded on the Magnetic Stripe does not indicate the presence of a Chip. - A Transaction for which the Authorization Request contains the CVV but either: – CVV verification was not performed – The Authorization record indicates that the CVV failed verification - A Transaction that was approved using a Payment Credential for which the Issuer had reported Fraud Activity - A Visa B2B Virtual Payments Program Transaction	**All**

Table 11-10: Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Invalid Disputes (continued)

Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud Invalid Disputes	Country/Region
A Transaction that contained a Token	**All excluding Europe**

ID# 0030235	**Edition: Apr 2020 | Last Updated: Apr 2020**

11.7.2.4   Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud according to the following time limit:

Table 11-11: Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Time Limit

Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**

ID# 0030236	**Edition: Apr 2020 | Last Updated: Apr 2018**

11.7.2.5   Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud:

Table 11-12: Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Dispute Processing Requirements

Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud Supporting Documentation/Certification	Country/Region
All of the following: • Certification that the Cardholder denies authorization of or participation in the Transaction • For key-entered Transactions, certification that the Card is a Chip Card	**All**

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

ID# 0030237   Edition: Apr 2020 | Last Updated: Apr 2019

11.7.2.6   Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud:

Table 11-13: Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud – Pre-Arbitration Processing Requirements

Dispute Condition 10.1: EMV Liability Shift Counterfeit Fraud Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. • The Dispute is invalid. • The Cardholder no longer disputes the Transaction.	**Effective for pre-Arbitration attempts processed through 17 April 2020** **All** **Effective for pre-Arbitration attempts processed on or after 18 April 2020** **All excluding US**
Effective for pre-Arbitration attempts processed on or after 18 April 2020 Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. • The Dispute is invalid. • The Cardholder no longer disputes the Transaction. • Compelling Evidence	**US**

ID# 0030238   Edition: Apr 2020 | Last Updated: Apr 2020

11.7.3   Dispute Condition 10.2: EMV Liability Shift – Non-Counterfeit Fraud

11.7.3.1   Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud for the following reason:

Table 11-14: Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Reasons

Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud Dispute Reasons	Country/Region

The Transaction qualifies for the EMV liability shift, as specified in *Section 1.11.1.2, EMV Liability Shift Participation*, and all of the following:
 	
• The Transaction was completed in a Card-Present Environment.
 	
• The Cardholder denies authorization of or participation in the Transaction.
 	
• The Card is a PIN-Preferring Chip Card.
 	
• One of the following:
 	
  – The Transaction did not take place at a Chip-Reading Device.
 	
  – A Chip-initiated Transaction took place at a Chip-Reading Device that was not EMV PIN-compliant.
 	
  – The Transaction was Chip-initiated without online PIN and both:
 	
    ▪ The Transaction was authorized Online
 	
    ▪ The Acquirer did not transmit the Full-Chip Data to Visa in the Authorization Request.
	All

ID# 0030239   Edition: Apr 2020 | Last Updated: Apr 2018

11.7.3.2   Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Rights

Table 11-15: Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Rights

Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud Dispute Rights	Country/Region
Before initiating a Dispute, an Issuer must report the Fraud Activity using fraud type code 0 (lost), 1 (stolen), or 2 (Card not received as issued [NRI]).	**All**

ID# 0030240   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.7.3.3   Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Invalid Disputes

A Dispute is invalid under Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud for any of the following:

Table 11-16: Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Invalid Disputes

Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud Invalid Disputes	Country/Region
- An ATM Cash Disbursement - A Contactless Transaction - An Emergency Cash Disbursement Transaction - A Mobile Push Payment Transaction - A Transaction where both an Imprint and a PIN were obtained - A Transaction that was correctly processed at an EMV PIN-Compliant Acceptance Device - A Visa Easy Payment Service (VEPS) Transaction - A Fallback Transaction - A Transaction that was approved using a Payment Credential for which the Issuer had reported Fraud Activity - A Visa B2B Virtual Payments Program Transaction - A Mass Transit Transaction	**All**

ID# 0030241	Edition: Apr 2020 | Last Updated: Apr 2020

11.7.3.4   Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud according to the following time limit:

Table 11-17: Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Time Limit

Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**

ID# 0030242	Edition: Apr 2020 | Last Updated: Apr 2018

11.7.3.5   Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud:

Table 11-18: Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Dispute Processing Requirements

Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud Supporting Documentation/Certification	Country/Region
Both: • Certification that the Card was a PIN-Preferring Chip Card • Certification that the Cardholder denies authorization of or participation in the Transaction	**All**

ID# 0030243	Edition: Apr 2020 | Last Updated: Apr 2019

11.7.3.6   Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud:

Table 11-19: Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud – Pre-Arbitration Processing Requirements

Dispute Condition 10.2: EMV Liability Shift Non-Counterfeit Fraud Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the merchant was not addressed by the Issuer in the Dispute. • The Dispute is invalid. • The Cardholder no longer disputes the Transaction.	All

ID# 0030244   Edition: Apr 2020 | Last Updated: Apr 2018

11.7.4   Dispute Condition 10.3: Other Fraud – Card-Present Environment

11.7.4.1   Dispute Condition 10.3: Other Fraud – Card-Present Environment – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 10.3: Other Fraud – Card-Present Environment for the following reason:

Table 11-20: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Dispute Reasons

Dispute Condition 10.3: Other Fraud – Card-Present Environment Dispute Reasons	Country/Region
The Cardholder denies authorization of or participation in a key-entered or Unattended Transaction conducted in a Card-Present Environment.	All

ID# 0030245   Edition: Apr 2020 | Last Updated: Apr 2018

11.7.4.2   Dispute Condition 10.3: Other Fraud – Card-Present Environment – Dispute Rights

Table 11-21: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Dispute Rights

Dispute Condition 10.3: Other Fraud – Card-Present Environment Dispute Rights	Country/Region
Before initiating a Dispute, an Issuer must report the Fraud Activity to Visa.	**All**

ID# 0030246   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.7.4.3   Dispute Condition 10.3: Other Fraud – Card-Present Environment – Invalid Disputes

A Dispute is invalid under Dispute Condition 10.3: Other Fraud – Card-Present Environment for any of the following:

Table 11-22: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Invalid Disputes

Dispute Condition 10.3: Other Fraud – Card-Present Environment Invalid Disputes	Country/Region
- An ATM Cash Disbursement - An Emergency Cash Disbursement Transaction - A Mobile Push Payment Transaction - A Transaction that was approved using a Payment Credential for which the Issuer had reported Fraud Activity - A Transaction where either of the following was obtained: - For a Face-to-Face Environment Transaction, an Electronic Imprint - For an Unattended Transaction, an Imprint and either a PIN or Consumer Device Cardholder Verification Method (CDCVM) - An Unattended Transaction that either: - Was an Online-authorized Chip-initiated Transaction[1] - Both: - Originated with a Counterfeit Card - Received an Approval Response that included POS Entry Mode code 05,	**All**

Table 11-22: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Invalid Disputes (continued)

Dispute Condition 10.3: Other Fraud – Card-Present Environment Invalid Disputes	Country/Region
07, 90, or 91 • A Visa Easy Payment Service Transaction • A Visa B2B Virtual Payment Program Transaction • A Payment Credential on which the Issuer reported Fraud Activity using fraud type code 3 (fraudulent application) • A Mass Transit Transaction	
An Unattended Transaction that is initiated with either a Magnetic Stripe-only Card or a Chip Card that is EMV Compliant and signature-preferring	**Europe**
[1] In the Europe Region: This does not apply to Transactions conducted at a UCAT that is not required to accept a PIN.	

ID# 0030247	Edition: Apr 2020 | Last Updated: Apr 2020

11.7.4.4   Dispute Condition 10.3: Other Fraud – Card Present Environment – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 10.3: Other Fraud – Card-Present Environment according to the following time limit:

Table 11-23: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Dispute Time Limit

Dispute Condition 10.3: Other Fraud – Card-Present Environment Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**

ID# 0030248	Edition: Apr 2020 | Last Updated: Apr 2018

11.7.4.5   Dispute Condition 10.3: Other Fraud – Card-Present Environment – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 10.3: Other Fraud – Card-Present Environment:

Table 11-24: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Dispute Processing Requirements

Dispute Condition 10.3: Other Fraud – Card-Present Environment Supporting Documentation/Certification	Country/Region
Certification that the Cardholder denies authorization of or participation in the Transaction	**All**

ID# 0030249   **Edition: Apr 2020 | Last Updated: Apr 2019**

11.7.4.6   Dispute Condition 10.3: Other Fraud – Card-Present Environment – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 10.3: Other Fraud – Card-Present Environment:

Table 11-25: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Pre-Arbitration Processing Requirements

Dispute Condition 10.3: Other Fraud – Card-Present Environment Supporting Documentation/Certification	Country/Region
Either: • Evidence that one of the following: – A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. – The Dispute is invalid. – The Cardholder no longer disputes the Transaction. – For a Transaction involving an initial Card-present Transaction and one or more ensuing key-entered Transactions, both: ▪ Evidence that all Transactions occurred during the same stay, trip, or rental period ▪ Evidence of an Imprint[1] for the initial Card-Present Environment Transaction • Both: – Evidence of an Imprint[1,2]	**Effective for pre-Arbitration attempts processed through 17 April 2020** **All** **Effective for pre-Arbitration attempts processed on or after 18 April 2020** **All excluding US**

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-25: Dispute Condition 10.3: Other Fraud – Card-Present Environment – Pre-Arbitration Processing Requirements (continued)

Dispute Condition 10.3: Other Fraud – Card-Present Environment Supporting Documentation/Certification	Country/Region
– For an Unattended Transaction, PIN or Consumer Device Cardholder Verification Method (CDCVM)	
Effective for pre-Arbitration attempts processed on or after 18 April 2020 Either: • Evidence of one of the following: – A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. – The Dispute is invalid. – The Cardholder no longer disputes the Transaction. – Compelling Evidence – For a Transaction involving an initial Card-present Transaction and one or more ensuing key-entered Transactions, both: ▪ Evidence that all Transactions occurred during the same stay, trip, or rental period ▪ Evidence of an Imprint[1] for the initial Card-Present Environment Transaction • Both: – Evidence of an Imprint[1] – For an Unattended Transaction, PIN or Consumer Device Cardholder Verification Method (CDCVM)	US
[1] A pencil rubbing or photocopy of a Card is not considered a valid Imprint. [2] In the Europe Region: This rule only applies to Unattended Transactions.	

ID# 0030250   **Edition: Apr 2020 | Last Updated: Apr 2020**

11.7.5   Dispute Condition 10.4: Other Fraud – Card-Absent Environment

11.7.5.1   Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 10.4: Other Fraud – Card-Absent Environment for the following reason:

Table 11-26: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Reasons

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Dispute Reasons	Country/Region
The Cardholder denies authorization of or participation in a Transaction conducted in a Card-Absent Environment.	**All**

ID# 0030252	Edition: Apr 2020 | Last Updated: Apr 2018

11.7.5.2   Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Rights

Table 11-27: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Rights

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Dispute Rights	Country/Region
• Before initiating a Dispute, an Issuer must report the Fraud Activity to Visa. • The Dispute applies to an Electronic Commerce Transaction in which the Issuer responded to an Authentication Request (PAReq[1]) with either: – An Unable-to-Authenticate Response (PARes[2] value U) or Authentication Denial (PARes value N) – A Cardholder Authentication Verification Value (CAVV) and Authentication Identifier, if the Acquirer did not provide a CAVV in the Authorization Request	**All**
For a Mail/Phone Order Transaction or an Electronic Commerce Transaction, the Dispute applies if the Issuer was unable to respond to an Address Verification Service Authorization Request because the Transaction was attempted with a Visa Commercial Card or a Card type where the Cardholder is anonymous.	**Canada Domestic**

Table 11-27: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Rights (continued)

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Dispute Rights	Country/Region
The Dispute applies, regardless of the Electronic Commerce Indicator value, for Electronic Commerce Transactions conducted by Merchants assigned the following MCCs: • 4829 (Wire Transfer Money Orders) • 5967 (Direct Marketing – Inbound Teleservices Merchant) • 6051 (Non-Financial Institutions – Foreign Currency, Non-Fiat Currency [for example: Cryptocurrency], Money Orders [not Money Transfer], Travelers Cheques, and Debt Repayment) • 6540 (Non-Financial Institutions: Stored Value Card Purchase/Load) • 7801 (Government Licensed On-Line Casinos [On-Line Gambling]) • 7802 (Government-Licensed Horse/Dog Racing) • 7995 (Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks)	US Domestic
¹ The "payer authentication request" message type, as specified in the *Visa Secure Program Guide* ² The "payer authentication response" message type, as specified in the *Visa Secure Program Guide*	

ID# 0030253   **Edition: Apr 2020 | Last Updated: Apr 2020**

11.7.5.3   Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Invalid Disputes

A Dispute is invalid under Dispute Condition 10.4: Other Fraud – Card-Absent Environment for any of the following:

Table 11-28: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Invalid Disputes

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Invalid Disputes	Country/Region
• An Emergency Cash Disbursement • A Straight Through Processing Transaction • A Transaction that was approved using a Payment Credential for which the	All

Table 11-28: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Invalid Disputes (continued)

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Invalid Disputes	Country/Region

Issuer had reported Fraud Activity
 	
• A Transaction on a Payment Credential for which the Issuer has initiated more than 35 Disputes[1] within the previous 120 calendar days
 	
• A Card-Absent Environment Transaction for which both:
 	
  – The CVV2 result code in the Authorization message is U (Issuer not participating in CVV2 program).
 	
  – The CVV2 presence indicator in the Authorization Request is one of the following:
 	
    ▪ 1 (CVV2 value is present)
 	
    ▪ 2 (CVV2 value is on the Card but is illegible)
 	
    ▪ 9 (Cardholder states CVV2 is not present on the Card)
 	
• A Mobile Push Payment Transaction
 	
• A Secure Electronic Commerce Transaction processed with Electronic Commerce Indicator value 5 in the Authorization Request, if all of the following:
 	
  – **Effective for Transactions completed through 15 October 2021** The Issuer responded to an Authentication Request with an Authentication Confirmation using Visa Secure.
 	
  – **Effective for Transactions completed on or after 16 October 2021** The Issuer responded to an Authentication Request with an Authentication Confirmation using Visa Secure with EMV 3-D Secure.
 	
  – The Cardholder Authentication Verification Value (CAVV) was included in the Authorization Request.
 	
• **Effective for Transactions completed through 15 October 2021** A Non-Authenticated Security Transaction processed using 3-D Secure 1.0 with Electronic Commerce Indicator value 6 if the Transaction is not a Non-Reloadable Prepaid Card Transaction and either:
 	
  – The Issuer, or Visa on behalf of the Issuer, responded to an Authentication Request with a non-participation message (VERes value N).
 	
  – Both:	

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-28: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Invalid Disputes (continued)

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Invalid Disputes	Country/Region

▪ The Issuer, or Visa on behalf of the Issuer, responded to an Authentication Request with an Attempt Response (PARes value A) using Visa Secure.
 	
▪ A Cardholder Authentication Verification Value (CAVV) was included in the Authorization Request.
 	
• A Non-Authenticated Security Transaction processed using 3-D Secure 2.0 with Electronic Commerce indicator value 6 in the Authorization Request, if all of the following apply:
 	
  – A Cardholder Authentication Verification Value (CAVV) was included in the Authorization Request.
 	
  – The Issuer, or Visa on behalf of the Issuer, responded to an Authentication Request with an Attempt Response using Visa Secure and a Cardholder Authentication Verification Value (CAVV) was included.
 	
  – The Transaction is not a Non-Reloadable Prepaid Card Transaction.
 	
• A Payment Credential on which the Issuer reported Fraud Activity using fraud type code 3 (fraudulent application)
 	
• A Visa B2B Virtual Payments Program Transaction	

All of the following: • The Card Verification Value 2 (CVV2) presence indicator in the Authorization Request is 1 (CVV2 value is present) • The CVV2 results code in the Authorization message is N (No match) • The Authorization request was approved	**All**
A Transaction for which an Authorization was obtained, if both: • The Acquirer attempted to authenticate the Cardholder through the Address Verification Service. • The Issuer is not an Address Verification Service participant.	**Canada Domestic**
• A Mail/Phone Order Transaction or an Electronic Commerce Transaction, if both: – The merchandise was shipped or delivered, or services were purchased.	**US Domestic**

Table 11-28: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Invalid Disputes (continued)

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Invalid Disputes	Country/Region
– The Issuer was not a participant in the Address Verification Service on the Transaction Date and the Acquirer received an Address Verification Service response code U. • An Airline or passenger railway Transaction, if either: – The Issuer response to an Address Verification Service inquiry was Y and tickets were mailed to the Cardholder billing address on the Issuer file. – The Issuer was not a participant in the Address Verification Service on the Transaction Date.	
• An AVS Result Code "U" and the Authorization contained address data	**UK Domestic**
¹ In the LAC Region (Brazil): This does not apply to a domestic Installment Transaction. The 35-Dispute limit applies based on the original Authorization.	

ID# 0030254   Edition: Apr 2020 | Last Updated: Apr 2020

11.7.5.4   Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 10.4: Other Fraud – Card-Absent Environment according to the following time limit:

Table 11-29: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Time Limit

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**

ID# 0030255   Edition: Apr 2020 | Last Updated: Apr 2018

11.7.5.5   Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 10.4: Other Fraud – Card-Absent Environment:

Table 11-30: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Dispute Processing Requirements

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Supporting Documentation/Certification	Country/Region
Certification that the Cardholder denies authorization of or participation in the Transaction	**All**

ID# 0030256   **Edition: Apr 2020 | Last Updated: Apr 2019**

11.7.5.6   Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 10.4: Other Fraud – Card-Absent Environment:

Table 11-31: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Pre-Arbitration Processing Requirements

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Supporting Documentation/Certification	Country/Region
One of the following: • Evidence that one of the following: – A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. – The Dispute is invalid. – The Cardholder no longer disputes the Transaction. • Compelling Evidence • For a Transaction involving an initial Card-present Transaction and one or more ensuing key-entered Transactions, both: – Evidence that all Transactions occurred during the same stay, trip, or	**All**

Table 11-31: Dispute Condition 10.4: Other Fraud – Card-Absent Environment – Pre-Arbitration Processing Requirements (continued)

Dispute Condition 10.4: Other Fraud – Card-Absent Environment Supporting Documentation/Certification	Country/Region
rental period – Evidence of a valid Imprint for the initial Card-Present Environment Transaction	

Either:
 	
• For an Airline Transaction, evidence that the Cardholder name is included in the manifest for the departed flight and matches the Cardholder name provided on the purchased itinerary
 	
• For a Transaction at a digital goods Merchant assigned MCC 5815 (Digital Goods – Media, Books, Movies, Music), 5816 (Games), 5817 (Applications [Excludes Games]) or 5818 (Digital Goods – Large Digital Goods Merchants), all of the following:
 	
  – Evidence that the Merchant has been successfully registered in and continues to participate in the Visa Digital Commerce Program
 	
  – Evidence that the Merchant is the owner of the operating system for the electronic device
 	
  – Evidence that the account set up on the Merchant's website or application was accessed by the Cardholder and was successfully verified by the Merchant before or on the Transaction Date
 	
  – Evidence that the disputed Transaction used the same device and Card as previous Transactions that were not disputed
 	
  – Evidence that the device ID number, IP address and geographic location, and name of device (if available) are linked to the Cardholder profile on record at the Merchant
 	
  – Description of the digital goods and the date and time they were purchased and successfully downloaded
 	
  – Customer name linked to the customer profile on record at the Merchant
 	
  – Evidence that the customer password was re-entered on the Merchant's website or application at the time of purchase
 	
  – Evidence that the Merchant validated the Card when the Cardholder first linked the Card to the customer profile on record at the Merchant
	All excluding Europe

ID# 0030257	Edition: Apr 2020 | Last Updated: Oct 2018

11.7.6   Dispute Condition 10.5: Visa Fraud Monitoring Program

11.7.6.1   Dispute Condition 10.5: Visa Fraud Monitoring Program – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 10.5: Visa Fraud Monitoring Program for the following reason:

Table 11-32: Dispute Condition 10.5: Visa Fraud Monitoring Program – Dispute Reasons

Dispute Condition 10.5: Visa Fraud Monitoring Program Dispute Reasons	Country/Region
Visa notified the Issuer that the Transaction was identified by the Visa Fraud Monitoring Program and the Issuer has not successfully disputed the Transaction under another Dispute condition.	**All**

ID# 0030258	Edition: Apr 2020 | Last Updated: Apr 2018

11.7.6.2   Dispute Condition 10.5: Visa Fraud Monitoring Program – Invalid Disputes

A Dispute is invalid under Dispute Condition 10.5: Visa Fraud Monitoring Program for the following:

Table 11-33: Dispute Condition 10.5 Visa Fraud Monitoring Program – Invalid Disputes

Dispute Condition 10.5: Visa Fraud Monitoring Program Invalid Disputes	Country/Region
None	**All**

ID# 0030626	Edition: Apr 2020 | Last Updated: Apr 2020

11.7.6.3   Dispute Condition 10.5: Visa Fraud Monitoring Program – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 10.5: Visa Fraud Monitoring Program according to the following time limit:

Table 11-34: Dispute Condition 10.5: Visa Fraud Monitoring Program – Dispute Time Limit

Dispute Condition 10.5: Visa Fraud Monitoring Program Dispute Time Limit	Country/Region
120 calendar days from the date of identification by the Visa Fraud Monitoring Program	**All**

ID# 0030259   Edition: Apr 2020 | Last Updated: Apr 2018

11.7.6.4   Dispute Condition 10.5: Visa Fraud Monitoring Program – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 10.5: Visa Fraud Monitoring Program:

Table 11-35: Dispute Condition 10.5: Visa Fraud Monitoring Program – Pre-Arbitration Processing Requirements

Dispute Condition 10.5: Visa Fraud Monitoring Program Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. • The Dispute is invalid. • The Cardholder no longer disputes the Transaction.	**All**

ID# 0030260   Edition: Apr 2020 | Last Updated: Apr 2018

11.8   Dispute Category 11: Authorization

11.8.1   Dispute Condition 11.1: Card Recovery Bulletin

11.8.1.1   Dispute Condition 11.1: Card Recovery Bulletin – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 11.1: Card Recovery Bulletin for the following reason:

Table 11-36: Dispute Condition 11.1: Card Recovery Bulletin – Dispute Reasons

Dispute Condition 11.1: Card Recovery Bulletin Dispute Reasons	Country/Region
All of the following: • The Transaction was below the Merchant's Floor Limit. • The Merchant did not obtain Authorization. • On the Transaction Date, the Account Number was listed in the Card Recovery Bulletin for the Visa Region in which the Merchant Outlet is located.[1,2]	**All**
[1] The Dispute applies even if a specific Account Number in a blocked BIN does not appear in the Card Recovery Bulletin. [2] If the Transaction Date was not transmitted in the Clearing Record, the Dispute applies if the Account Number was listed in the Card Recovery Bulletin within the 10 calendar days before the Transaction Processing Date.	

ID# 0030261   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.8.1.2   Dispute Condition 11.1: Card Recovery Bulletin – Invalid Disputes

A Dispute is invalid under Dispute Condition 11.1: Card Recovery Bulletin for the following:

Table 11-37: Dispute Condition 11.1: Card Recovery Bulletin – Invalid Disputes

Dispute Condition 11.1: Card Recovery Bulletin Invalid Disputes	Country/Region

• An ATM Cash Disbursement
 	
• A Mobile Push Payment Transaction
 	
• A Transaction completed at a Contactless-Only Acceptance Device
 	
• A Transaction that both:
 	
  – Occurred at a Chip-Reading Device
 	
  – Qualifies for the EMV liability shift, as specified in *Section 1.11.1.2, EMV Liability Shift Participation*
	All

ID# 0030262   **Edition: Apr 2020 | Last Updated: Apr 2019**

11.8.1.3   Dispute Condition 11.1: Card Recovery Bulletin – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 11.1: Card Recovery Bulletin according to the following time limits:

Table 11-38: Dispute Condition 11.1: Card Recovery Bulletin – Dispute Time Limit

Dispute Condition 11.1: Card Recovery Bulletin Dispute Time Limit	Country/Region
75 calendar days from the Transaction Processing Date	**All**

ID# 0030263   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.8.1.4   Dispute Condition 11.1: Card Recovery Bulletin – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 11.1: Card Recovery Bulletin:

Table 11-39: Dispute Condition 11.1: Card Recovery Bulletin – Pre-Arbitration Processing Requirements

Dispute Condition 11.1: Card Recovery Bulletin Supporting Documentation/Certification	Country/Region

Either:
 	
• Evidence that one of the following:
 	
  – A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute.
 	
  – The Dispute is invalid.
 	
  – **Effective for Disputes processed through 19 April 2020** The Cardholder no longer disputes the Transaction.
 	
• For a dispute involving a Transaction at a Car Rental Merchant, a Cruise Line Merchant, or a Lodging Merchant for which multiple Authorizations were obtained, evidence that the Account Number was not listed on the Card Recovery Bulletin on the following dates, as applicable:
 	
  – For a Lodging Merchant, the check-in date
 	
  – For a Car Rental Merchant, the vehicle rental date
 	
  – For a Cruise Line, the embarkation date
	All

ID# 0030264	Edition: Apr 2020 | Last Updated: Apr 2020

11.8.2   Dispute Condition 11.2: Declined Authorization

11.8.2.1   Dispute Condition 11.2: Declined Authorization – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 11.2: Declined Authorization for the following reason:

Table 11-40: Dispute Condition 11.2: Declined Authorization – Dispute Reasons

Dispute Condition 11.2: Declined Authorization Dispute Reasons	Country/Region
An Authorization Request received a Decline Response or Pickup Response and the Merchant completed the Transaction.	**All**

ID# 0030265	Edition: Apr 2020 | Last Updated: Apr 2018

11.8.2.2   Dispute Condition 11.2: Declined Authorization – Dispute Rights

Table 11-41: Dispute Condition 11.2: Declined Authorization – Dispute Rights

Dispute Condition 11.2: Declined Authorization Dispute Rights	Country/Region
A Dispute of a Mass Transit Transaction is valid for the full Transaction amount if a Decline Response was sent and the Transaction amount was greater than the amount specified in *Section 5.9.18.2, Mass Transit Transaction Requirements*	**All**

ID# 0030266	Edition: Apr 2020 | Last Updated: Apr 2018

11.8.2.3   Dispute Condition 11.2: Declined Authorization – Invalid Disputes

A Dispute is invalid under Dispute Condition 11.2: Declined Authorization for either of the following:

Table 11-42: Dispute Condition 11.2: Declined Authorization – Invalid Disputes

Dispute Condition 11.2: Declined Authorization Invalid Disputes	Country/Region
• An ATM Cash Disbursement • A Mobile Push Payment Transaction • A Transaction for which Authorization was obtained after a Decline Response was received for the same purchase. This does not include an Authorization Request that received a Pickup Response 04, 07, 41, or 43.	**All**

ID# 0030267	Edition: Apr 2020 | Last Updated: Apr 2019

11.8.2.4   Dispute Condition 11.2: Declined Authorization – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 11.2: Declined Authorization according to the following time limits:

Table 11-43: Dispute Condition 11.2: Declined Authorization – Dispute Time Limit

Dispute Condition 11.2: Declined Authorization Dispute Time Limit	Country/Region
75 calendar days from the Transaction Processing Date	**All**

ID# 0030268	Edition: Apr 2020 | Last Updated: Apr 2018

11.8.2.5   Dispute Condition 11.2: Declined Authorization – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 11.2: Declined Authorization:

Table 11-44: Dispute Condition 11.2: Declined Authorization – Pre-Arbitration Processing Requirements

Dispute Condition 11.2: Declined Authorization Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer	**All**

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-44: Dispute Condition 11.2: Declined Authorization – Pre-Arbitration Processing Requirements (continued)

Dispute Condition 11.2: Declined Authorization Supporting Documentation/Certification	Country/Region

in the Dispute
 	
• The Dispute is invalid
 	
• **Effective for Disputes processed through 19 April 2020** The Cardholder no longer disputes the Transaction
 	
• The Transaction was Chip-initiated and offline-authorized, if applicable
 	
• For a dispute involving a Transaction at a Car Rental Merchant, a Cruise Line Merchant, or a Lodging Merchant for which multiple Authorizations were obtained, certification of all of the following:
 	
  – The check-in date, embarkation date, or vehicle rental date
 	
  – The check-out date, disembarkation date, or vehicle return date
 	
  – The dates, authorized amounts, and Authorization Codes of the approved Authorizations	

ID# 0030269	Edition: Apr 2020 | Last Updated: Apr 2020

11.8.3   Dispute Condition 11.3: No Authorization

11.8.3.1   Dispute Condition 11.3: No Authorization – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 11.3: No Authorization for the following reason:

Table 11-45: Dispute Condition 11.3: No Authorization – Dispute Reasons

Dispute Condition 11.3: No Authorization Dispute Reasons	Country/Region
Authorization was required but was not obtained on the date specified in *Section 5.8.4.5, Approval Response Validity Timeframes*	**All**

ID# 0030270	Edition: Apr 2020 | Last Updated: Apr 2018

11.8.3.2   Dispute Condition 11.3: No Authorization – Dispute Rights

Table 11-46: Dispute Condition 11.3: No Authorization – Dispute Rights

Dispute Condition 11.3: No Authorization Dispute Rights	Country/Region

• The Dispute is limited to the amount above the applicable Floor Limit for a Chip-initiated, Offline-Authorized Transaction.
 	
• If Authorization was obtained for an amount less than the Transaction amount, the Dispute is limited to either:
 	
  – The amount that was not authorized
 	
  – The difference between the Transaction amount and the amount for which Authorization was required, as specified in *Section 5.8.3.1, Authorization Amount Requirements*
 	
• The Dispute applies to a Chip-initiated Transaction that included an Authorization Request Cryptogram (ARQC) in the Clearing Record but was not authorized Online by the Issuer or the Issuer's agent.
	All

ID# 0030271	Edition: Apr 2020 | Last Updated: Apr 2018

11.8.3.3   Dispute Condition 11.3: No Authorization – Invalid Disputes

A Dispute is invalid under Dispute Condition 11.3: No Authorization for any of the following:

Table 11-47: Dispute Condition 11.3: No Authorization – Invalid Disputes

Dispute Condition 11.3: No Authorization Invalid Disputes	Country/Region
• An ATM Cash Disbursement • A Transaction for which valid Authorization was obtained • An Electronic Commerce Transaction in which the Cardholder Authentication Verification Value (CAVV) was not validated during Authorization • A Mobile Push Payment Transaction • **Effective for Transactions completed through 17 April 2020** A Credit Transaction • **Effective for Transactions completed on or after 18 April 2020** A Credit	**All**

Table 11-47: Dispute Condition 11.3: No Authorization – Invalid Disputes (continued)

Dispute Condition 11.3: No Authorization Invalid Disputes	Country/Region
Transaction with one of the following MCCs: – 3000-3350 (Airlines, Air Carriers) – 4111 (Local and Suburban Commuter Passenger Transportation, Including Ferries) – 4112 (Passenger Railways) – 4131 (Bus Lines) – 4511 (Airlines and Air Carriers [Not Elsewhere Classified])	
A Transaction that both: • Is processed with a Visa Drive Card that is an "extra" Card which has a Privately Contracted Agreement associated to it • Contains either of the following MCCs: – 4784 (Tolls and Bridge Fees) – 7523 (Parking Lots, Parking Meters and Garages)	**Europe**

ID# 0030272   Edition: Apr 2020 | Last Updated: Apr 2020

11.8.3.4   Dispute Condition 11.3: No Authorization – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 11.3: No Authorization according to the following time limits:

Table 11-48: Dispute Condition 11.3: No Authorization – Dispute Time Limit

Dispute Condition 11.3: No Authorization Dispute Time Limit	Country/Region
75 calendar days from the Transaction Processing Date	**All**

ID# 0030273   Edition: Apr 2020 | Last Updated: Apr 2018

11.8.3.5   Dispute Condition 11.3: No Authorization – Pre-Arbitration Processing Requirements

An Acquirer must provide the following documentation or certification for a pre-Arbitration attempt under Dispute Condition 11.3: No Authorization:

Table 11-49: Dispute Condition 11.3: No Authorization – Pre-Arbitration Processing Requirements

Dispute Condition 11.3: No Authorization Supporting Documentation/Certification	Country/Region
Both: • Evidence of any of the following: – A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. – The Dispute is invalid. – **Effective for Disputes processed through 19 April 2020** The Cardholder no longer disputes the Transaction. – The Transaction Date in the Clearing Record was incorrect and the Authorization was obtained on the correct date. • For a dispute involving special Authorization procedures where all of the following apply: – The first Authorization Request included the initial/Estimated Authorization Request indicator. – Subsequent Authorization Requests included the Incremental Authorization Request indicator. – The same Transaction Identifier was used in all Authorization Requests. – Clearing Records were submitted within the timeframes specified in *Section 5.8.4.5, Approval Response Validity Timeframes*. Both: – The Transaction Receipt or Substitute Transaction Receipt – Certification of all of the following: ▪ The date the Transaction was initiated ▪ The date the Transaction was completed ▪ The dates, authorized amounts, and Authorization Codes of the	All

Table 11-49: Dispute Condition 11.3: No Authorization – Pre-Arbitration Processing Requirements (continued)

Dispute Condition 11.3: No Authorization Supporting Documentation/Certification	Country/Region
approved Authorizations	

ID# 0030274	Edition: Apr 2020 | Last Updated: Apr 2020

11.9   Dispute Category 12: Processing Errors

11.9.1   Dispute Condition 12.1: Late Presentment

11.9.1.1   Dispute Condition 12.1: Late Presentment – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 12.1: Late Presentment for the following reasons:

Table 11-50: Dispute Condition 12.1: Late Presentment – Dispute Reasons

Dispute Condition 12.1: Late Presentment Dispute Reasons	Country/Region

Either:[1]
 	
• The Transaction Date is more than 180 calendar days before the Transaction Processing Date.
• Both:
  – The Transaction was not processed within the required time limit as specified in *Section 7.7.1.1, Acquirer Processing Timeframes*.
  – The Transaction was processed to a "closed," "credit problem," or "fraud" account.
	All

The Acquirer processed an Adjustment of a Shared Deposit Transaction and either: • The Shared Deposit Adjustment posted to a "closed" or "credit problem" account and the Adjustment was processed more than 10 days after the Transaction Date. • The Shared Deposit Adjustment, was processed more than 45 days after the	**All**

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-50: Dispute Condition 12.1: Late Presentment – Dispute Reasons (continued)

Dispute Condition 12.1: Late Presentment Dispute Reasons	Country/Region
Transaction Date.	
Effective for Adjustments processed through 17 April 2020 The Acquirer processed an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit Transaction and either: • The Adjustment posted to a "closed," "credit problem," or "fraud" account and the Adjustment was processed more than 10 days after the Transaction Date. • The Adjustment was processed more than 45 days after the Transaction Date.	**US Domestic**
Effective for Adjustments processed on or after 18 April 2020 The Acquirer processed an Adjustment of an ATM Cash Disbursement[2] and either: • The Adjustment posted to a "closed," "credit problem," or "fraud" account and the Adjustment was processed more than 10 days after the Transaction Date. • The Adjustment was processed more than 45 days after the Transaction Date.	**All excluding India Domestic**
Effective for Adjustments processed through 31 October 2019 The Acquirer processed an Adjustment of an ATM Cash Disbursement more than 5 days after the Transaction Date and the Adjustment was posted to a "closed," "credit problem," or "fraud" account. **Effective for Adjustments processed on or after 1 November 2019** The Acquirer processed an Adjustment of an ATM Cash Disbursement more than 4 days after the Transaction Date and the Adjustment was posted to a "closed," "credit problem," or "fraud" account.	**India Domestic**

[1] In the LAC Region (Brazil): For a domestic Installment Transaction, the Transaction was processed between the Transaction Date and the Processing Date of the first Installment Transaction.

[2] In the US Region: For US Domestic Transaction, this includes Adjustment of a PIN-Authenticated Visa Debit Transaction.

ID# 0030275   Edition: Apr 2020 | Last Updated: Apr 2020

11.9.1.2   Dispute Condition 12.1: Late Presentment – Dispute Rights

Table 11-51: Dispute Condition 12.1: Late Presentment – Dispute Rights

Dispute Condition 12.1: Late Presentment Dispute Rights	Country/Region
For the purpose of this condition, the Transaction Date refers to the Transaction Date transmitted in the Clearing Record.	**All**

ID# 0030276	**Edition: Apr 2020 | Last Updated: Apr 2018**

11.9.1.3   Dispute Condition 12.1: Late Presentment – Invalid Disputes

A Dispute is invalid under Dispute Condition 12.1: Late Presentment for any of the following:

Table 11-52: Dispute Condition 12.1: Late Presentment – Invalid Disputes

Dispute Condition 12.1: Late Presentment Invalid Disputes	Country/Region
A Mobile Push Payment Transaction	**All**

ID# 0030550	**Edition: Apr 2020 | Last Updated: Apr 2019**

11.9.1.4   Dispute Condition 12.1: Late Presentment – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 12.1: Late Presentment according to the following time limits:

Table 11-53: Dispute Condition 12.1: Late Presentment – Dispute Time Limit

Dispute Condition 12.1: Late Presentment Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**
120 calendar days from either: • The Transaction Processing Date • For an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit Transaction, the Transaction Date of the Adjustment	**US Domestic**

Table 11-53: Dispute Condition 12.1: Late Presentment – Dispute Time Limit (continued)

Dispute Condition 12.1: Late Presentment Dispute Time Limit	Country/Region
120 calendar days from either: • The Transaction Processing Date • For an Adjustment of an ATM Cash Disbursement, the Transaction Date of the Adjustment	**India Domestic**

ID# 0030277	Edition: Apr 2020 | Last Updated: Apr 2019

11.9.1.5   Dispute Condition 12.1: Late Presentment – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 12.1: Late Presentment:

Table 11-54: Dispute Condition 12.1: Late Presentment – Dispute Processing Requirements

Dispute Condition 12.1: Late Presentment Supporting Documentation/Certification	Country/Region

Certification that either:
 	
• On the Dispute Processing Date, the Cardholder account status was flagged as one of the following:
  – Credit Problem
  – Closed
  – Fraud[1]
• The Transaction was processed more than 180 calendar days after the Transaction Date.
	All

[1] This does not apply to Shared Deposit Transactions.	

ID# 0030278	Edition: Apr 2020 | Last Updated: Apr 2019

11.9.1.6   Dispute Condition 12.1: Late Presentment – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 12.1: Late Presentment:

Table 11-55: Dispute Condition 12.1: Late Presentment – Dispute Response Processing Requirements

Dispute Condition 12.1: Late Presentment Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • The Transaction Receipt or other record with a Transaction Date that disproves late Presentment and proves that the Acquirer obtained the required authorization	**All**

ID# 0030279	**Edition: Apr 2020	Last Updated: Apr 2019**

11.9.2   Dispute Condition 12.2: Incorrect Transaction Code

11.9.2.1   Dispute Condition 12.2: Incorrect Transaction Code – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 12.2: Incorrect Transaction Code for the following reasons:

Table 11-56: Dispute Condition 12.2: Incorrect Transaction Code – Dispute Reasons

Dispute Condition 12.2: Incorrect Transaction Code Dispute Reasons	Country/Region
One of the following: • A credit was processed as a debit. • A debit was processed as a credit. • A credit refund was processed instead of a Reversal or an Adjustment.	**All**

ID# 0030280	Edition: Apr 2020	Last Updated: Apr 2018

11.9.2.2   Dispute Condition 12.2: Incorrect Transaction Code – Dispute Rights

Table 11-57: Dispute Condition 12.2: Incorrect Transaction Code – Dispute Rights

Dispute Condition 12.2: Incorrect Transaction Code Dispute Rights	Country/Region

• The Dispute amount should be double the Transaction amount if either:
  – A credit was processed as a debit.
  – A debit was processed as a credit.
• For a credit refund that was processed instead of a Reversal or an Adjustment, the Dispute amount is limited to the difference between the credit refund and the original debit.
	All

ID# 0030281	Edition: Apr 2020	Last Updated: Apr 2018

11.9.2.3   Dispute Condition 12.2: Incorrect Transaction Code – Invalid Disputes

A Dispute is invalid under Dispute Condition 12.2: Incorrect Transaction Code for any of the following:

Table 11-58: Dispute Condition 12.2: Incorrect Transaction Code – Invalid Disputes

Dispute Condition 12.2: Incorrect Transaction Code Invalid Disputes	Country/Region
A Mobile Push Payment Transaction	All

ID# 0030551	Edition: Apr 2020	Last Updated: Apr 2019

11.9.2.4   Dispute Condition 12.2: Incorrect Transaction Code – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 12.2: Incorrect Transaction Code according to the following time limits:

Table 11-59: Dispute Condition 12.2: Incorrect Transaction Code – Dispute Time Limit

Dispute Condition 12.2: Incorrect Transaction Code Dispute Time Limit	Country/Region
120 calendar days from either: • The Transaction Processing Date • For a credit refund that was processed instead of a Reversal or an Adjustment, the Processing Date of the credit refund	All

ID# 0030282   Edition: Apr 2020 | Last Updated: Apr 2018

11.9.2.5   Dispute Condition 12.2: Incorrect Transaction Code – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 12.2: Incorrect Transaction Code:

Table 11-60: Dispute Condition 12.2: Incorrect Transaction Code – Dispute Processing Requirements

Dispute Condition 12.2: Incorrect Transaction Code Supporting Documentation/Certification	Country/Region
Certification that either: • Credit was processed as a debit. • Debit was processed as a credit. For a credit refund that was processed instead of a Reversal or an Adjustment, both: • An explanation of why the credit refund was processed in error • Date of the original Transaction and Credit Transaction	All

ID# 0030283   Edition: Apr 2020 | Last Updated: Apr 2018

11.9.2.6   Dispute Condition 12.2: Incorrect Transaction Code – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 12.2: Incorrect Transaction Code:

Table 11-61: Dispute Condition 12.2: Incorrect Transaction Code – Dispute Response Processing Requirements

Dispute Condition 12.2: Incorrect Transaction Code Supporting Documentation/Certification	Country/Region

Either:
 	
• For a credit processed as a debit or a debit processed as a credit, either:
 	
  – Evidence that a credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute
 	
  – Transaction Receipt or other record that proves that the Transaction code was correct
 	
• For a credit refund that was processed instead of a Reversal or an Adjustment, either:
 	
  – Evidence that a Reversal issued by the Merchant was not addressed by the Issuer in the Dispute
 	
  – A reason that a Credit Transaction was processed instead of a Reversal or an Adjustment
	All

ID# 0030284   Edition: Apr 2020 | Last Updated: Apr 2018

11.9.3   Dispute Condition 12.3: Incorrect Currency

11.9.3.1   Dispute Condition 12.3: Incorrect Currency – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 12.3: Incorrect Currency for the following reasons:

Table 11-62: Dispute Condition 12.3: Incorrect Currency – Dispute Reasons

Dispute Condition 12.3: Incorrect Currency Dispute Reasons	Country/Region
Either: • The Transaction Currency is different than the currency transmitted through VisaNet. • Dynamic Currency Conversion (DCC) occurred and the Cardholder did not agree to DCC and did not make an active choice or was refused the choice of paying in the Merchant's local currency or the selected ATM currency.	**All**

ID# 0030285	Edition: Apr 2020 | Last Updated: Apr 2019

11.9.3.2   Dispute Condition 12.3: Incorrect Currency – Dispute Rights

Table 11-63: Dispute Condition 12.3: Incorrect Currency – Dispute Rights

Dispute Condition 12.3: Incorrect Currency Dispute Rights	Country/Region
The Dispute applies for the entire Transaction amount.	**All**

ID# 0030286	Edition: Apr 2020 | Last Updated: Apr 2018

11.9.3.3   Dispute Condition 12.3: Incorrect Currency – Invalid Disputes

A Dispute is invalid under Dispute Condition 12.3: Incorrect Currency for the following:

Table 11-64: Dispute Condition 12.3: Incorrect Currency – Invalid Disputes

Dispute Condition 12.3: Incorrect Currency Invalid Disputes	Country/Region
• A Straight Through Processing Transaction • A Mobile Push Payment Transaction • A Transaction settled in USD originating at an ATM that is located outside the US Region and is connected to the Plus System. This does not include a DCC Transaction.	**All**

ID# 0030287   Edition: Apr 2020 | Last Updated: Apr 2019

11.9.3.4   Dispute Condition 12.3: Incorrect Currency – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 12.3: Incorrect Currency according to the following time limit:

Table 11-65: Dispute Condition 12.3: Incorrect Currency – Dispute Time Limit

Dispute Condition 12.3: Incorrect Currency Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**

ID# 0030288   Edition: Apr 2020 | Last Updated: Apr 2018

11.9.3.5   Dispute Condition 12.3: Incorrect Currency – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 12.3: Incorrect Currency:

Table 11-66: Dispute Condition 12.3: Incorrect Currency – Dispute Processing Requirements

Dispute Condition 12.3: Incorrect Currency Supporting Documentation/Certification	Country/Region
Either: • Certification stating the correct Transaction currency code • Certification that the Cardholder did not agree to Dynamic Currency Conversion and did not make an active choice or was refused the choice of paying in the Merchant's local currency or the selected ATM currency	**All**

ID# 0030289   Edition: Apr 2020 | Last Updated: Apr 2019

11.9.3.6   Dispute Condition 12.3: Incorrect Currency – Dispute Response Rights

Table 11-67: Dispute Condition 12.3: Incorrect Currency – Dispute Response Rights

Dispute Condition 12.3: Incorrect Currency Supporting Documentation/Certification	Country/Region
For a Dynamic Currency Conversion (DCC) Transaction, if the Acquirer cannot provide evidence of active choice by the Cardholder, it may either: • Process a Dispute Response in the Merchant's local currency, or the currency selected at the ATM, for the Transaction amount before DCC occurred, excluding fees or commission charges directly related to DCC that were applied to the Transaction. • Process the Transaction as a first Presentment instead of processing a Dispute Response. The Acquirer may be responsible for a Dispute for late Presentment.	**All**

ID# 0030290   **Edition: Apr 2020 | Last Updated: Apr 2019**

11.9.3.7   Dispute Condition 12.3: Incorrect Currency – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 12.3: Incorrect Currency:

Table 11-68: Dispute Condition 12.3: Incorrect Currency – Dispute Response Processing Requirements

Dispute Condition 12.3: Incorrect Currency Supporting Documentation/Certification	Country/Region

• Evidence that one of the following:
 	
  – A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute.
 	
  – The Dispute is invalid.
 	
  – The Cardholder no longer disputes the Transaction.
 	
• Transaction Receipt or other record that proves that the Transaction currency was correct
 	
• For a DCC Transaction, either:
	All

Table 11-68: Dispute Condition 12.3: Incorrect Currency – Dispute Response Processing Requirements (continued)

Dispute Condition 12.3: Incorrect Currency Supporting Documentation/Certification	Country/Region

– For a Dispute Response in the Merchant's local currency or the ATM dispensed currency, both:
  ▪ Acquirer certification that the Merchant is registered to offer DCC
  ▪ A copy of the Transaction Receipt showing the Merchant's local currency or the currency selected at the ATM
– For a Dispute Response in the DCC currency, all of the following:
  ▪ Evidence that the Cardholder actively chose DCC
  ▪ Acquirer certification that the Acceptance Device requires electronic selection of DCC by the Cardholder and that the choice cannot be made by the Merchant or ATM
  ▪ A copy of the Transaction Receipt	

ID# 0030291	Edition: Apr 2020 | Last Updated: Apr 2019

11.9.4   Dispute Condition 12.4: Incorrect Account Number

11.9.4.1   Dispute Condition 12.4: Incorrect Account Number – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 12.4: Incorrect Account Number for the following reason:

Table 11-69: Dispute Condition 12.4: Incorrect Account Number – Dispute Reasons

Dispute Condition 12.4: Incorrect Account Number Dispute Reasons	Country/Region
Either: • The Transaction or Original Credit Transaction was processed using an incorrect Payment Credential.[1] • A Shared Deposit Adjustment was processed using an incorrect Payment Credential.	**All**
[1] In the US Region: Includes an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit	

Table 11-69: Dispute Condition 12.4: Incorrect Account Number – Dispute Reasons (continued)

Dispute Condition 12.4: Incorrect Account Number Dispute Reasons	Country/Region
Transaction	

ID# 0030292	Edition: Apr 2020 | Last Updated: Apr 2020

11.9.4.2   Dispute Condition 12.4: Incorrect Account Number – Invalid Disputes

A Dispute is invalid under Dispute Condition 12.4: Incorrect Account Number for the following:

Table 11-70: Dispute Condition 12.4: Incorrect Account Number – Invalid Disputes

Dispute Condition 12.4: Incorrect Account Number Invalid Disputes	Country/Region
• An ATM Cash Disbursement • A Straight Through Processing Transaction • A Transaction using a Payment Credential for which no valid Card was issued or is outstanding and for which either an Imprint or an Authorization was obtained • A Chip-initiated Transaction containing a valid Cryptogram • A Mass Transit Transaction • A Mobile Push Payment Transaction	**All**

ID# 0030293	Edition: Apr 2020 | Last Updated: Apr 2020

11.9.4.3   Dispute Condition 12.4: Incorrect Account Number – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 12.4: Incorrect Account Number according to the following time limits:

Table 11-71: Dispute Condition 12.4: Incorrect Account Number – Dispute Time Limit

Dispute Condition 12.4: Incorrect Account Number Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**
120 calendar days from the Transaction Processing Date of a Shared Deposit Adjustment	**All**
120 calendar days from either: • The Transaction Processing Date • For an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit Transaction, the Transaction Date of the Adjustment	**US Domestic**

ID# 0030294   Edition: Apr 2020 | Last Updated: Apr 2019

11.9.4.4   Dispute Condition 12.4: Incorrect Account Number – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 12.4: Incorrect Account Number:

Table 11-72: Dispute Condition 12.4: Incorrect Account Number – Dispute Processing Requirements

Dispute Condition 12.4: Incorrect Account Number Supporting Documentation/Certification	Country/Region
Either: • Certification that the incorrect Payment Credential was used. • Certification that a Transaction was processed to a Payment Credential that does not match any Payment Credential on the Issuer's master file and no Authorization was obtained.	**All**

ID# 0030546   Edition: Apr 2020 | Last Updated: Apr 2020

11.9.4.5   Dispute Condition 12.4: Incorrect Account Number – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 12.4: Incorrect Account Number:

Table 11-73: Dispute Condition 12.4: Incorrect Account Number – Dispute Response Processing Requirements

Dispute Condition 12.4: Incorrect Account Number Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • Transaction Receipt or other record to prove that the Payment Credential was processed correctly	**All**

ID# 0030295	Edition: Apr 2020	Last Updated: Apr 2020

11.9.5   Dispute Condition 12.5 Incorrect Amount

11.9.5.1   Dispute Condition 12.5: Incorrect Amount – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 12.5: Incorrect Amount for the following reason:

Table 11-74: Dispute Condition 12.5: Incorrect Amount – Dispute Reasons

Dispute Condition 12.5: Incorrect Amount Dispute Reasons	Country/Region
Either: • The Transaction amount is incorrect or an addition or transposition error occurred. • For an ATM Transaction, the Shared Deposit Adjustment amount is incorrect.	**All**

ID# 0030296	Edition: Apr 2020	Last Updated: Apr 2019

11.9.5.2   Dispute Condition 12.5: Incorrect Amount – Dispute Rights

Table 11-75: Dispute Condition 12.5: Incorrect Amount – Dispute Rights

Dispute Condition 12.5: Incorrect Amount Dispute Rights	Country/Region
• The Dispute amount is limited to the difference between the amounts. • For an incorrect Transaction amount, if a handwritten Transaction amount differs from the imprinted amount, the handwritten amount must be used to determine the processing error.	**All**

ID# 0030297	Edition: Apr 2020	Last Updated: Apr 2018

11.9.5.3   Dispute Condition 12.5: Incorrect Amount – Invalid Disputes

A Dispute is invalid under Dispute Condition 12.5: Incorrect Amount for any of the following:

Table 11-76: Dispute Condition 12.5: Incorrect Amount – Invalid Disputes

Dispute Condition 12.5: Incorrect Amount Invalid Disputes	Country/Region
• An ATM Cash Disbursement • A Mobile Push Payment Transaction • A Straight Through Processing Transaction • A T&E Transaction in which there is a difference between the quoted price and the actual charges made by the Merchant • A No-Show Transaction • An Advance Payment[1] • A Transaction for which the Merchant has the right to alter the Transaction amount without the Cardholder's consent after the Transaction was completed	**All**
[1] Processed as specified in *Section 5.9.10.1, Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials*	

ID# 0030298	Edition: Apr 2020	Last Updated: Apr 2020

11.9.5.4 Dispute Condition 12.5: Incorrect Amount – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 12.5: Incorrect Amount according to the following time limits:

Table 11-77: Dispute Condition 12.5: Incorrect Amount – Dispute Time Limit

Dispute Condition 12.5: Incorrect Amount Dispute Time Limit	Country/Region
Either: • 120 calendar days from the Transaction Processing Date • 120 calendar days from the Transaction Processing Date of a Shared Deposit Adjustment	**All**
120 calendar days from either: • The Transaction Processing Date • For an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit Transaction, the Transaction Date of the Adjustment	**US Domestic**

ID# 0030299	Edition: Apr 2020	Last Updated: Apr 2019

11.9.5.5 Dispute Condition 12.5: Incorrect Amount – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 12.5: Incorrect Amount:

Table 11-78: Dispute Condition 12.5: Incorrect Amount – Dispute Processing Requirements

Dispute Condition 12.5: Incorrect Amount Supporting Documentation/Certification	Country/Region
• Certification of the correct Transaction Amount • For an ATM Transaction, certification of the correct Shared Deposit Adjustment amount	**All**

ID# 0030300	Edition: Apr 2020	Last Updated: Apr 2019

11.9.5.6   Dispute Condition 12.5: Incorrect Amount – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 12.5: Incorrect Amount:

Table 11-79: Dispute Condition 12.5: Incorrect Amount – Dispute Response Processing Requirements

Dispute Condition 12.5: Incorrect Amount Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Acquirer was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • Transaction Receipt or other record to prove that the Transaction amount was correct	All

ID# 0030301	Edition: Apr 2020	Last Updated: Apr 2019

11.9.6   Dispute Condition 12.6: Duplicate Processing/Paid by Other Means

11.9.6.1   Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 12.6: Duplicate Processing/Paid by Other Means for the following reason:

Table 11-80: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Reasons

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Dispute Reasons	Country/Region
One of the following: • A single Transaction[1] was processed more than once using the same Payment Credential.	All

Table 11-80: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Reasons (continued)

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Dispute Reasons	Country/Region
• The Cardholder[2] paid for the same merchandise or service by other means. • For an ATM Transaction, a Shared Deposit Adjustment was processed more than once.	
[1] In the US Region: Includes an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit Transaction [2] Or Virtual Account holder	

ID# 0030302   **Edition: Apr 2020 | Last Updated: Apr 2020**

11.9.6.2   Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Rights

Table 11-81: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Rights

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Dispute Rights	Country/Region
For Duplicate Processing: • If the Transaction was processed by different Acquirers (including Originating Acquirers), the Acquirer that processed the invalid Transaction is responsible for the Dispute. If the Issuer (including a Recipient Issuer) cannot determine which Transaction is invalid, the Acquirer that processed the second Transaction is responsible for the Dispute. • For an ATM Transaction that was processed by different Acquirers, the Acquirer that processed the invalid Shared Deposit Adjustment is responsible for the Dispute. If the Issuer or Recipient Member cannot determine which Transaction is invalid, the Acquirer that processed the second Transaction is responsible for the Dispute. For Transactions that were paid by other means: • The Dispute applies when a contract reflects that the Merchant accepted a voucher issued by a third party as payment for merchandise or for services rendered, and subsequently bills the Cardholder because the Merchant is	**All**

Table 11-81: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Rights (continued)

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Dispute Rights	Country/Region
unable to collect payment from the third party. ● The Cardholder must attempt to resolve the dispute with the Merchant or the Merchant's liquidator, if applicable, before the Issuer may initiate a Dispute.[1]	
[1] Does not apply to a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services	

ID# 0030303   Edition: Apr 2020 | Last Updated: Apr 2019

11.9.6.3   Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Invalid Disputes

A Dispute is invalid under Dispute Condition 12.6: Duplicate Processing/Paid by Other Means as follows:

Table 11-82: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Invalid Disputes

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Invalid Disputes	Country/Region
Transactions in which payment for services was made to different Merchants, unless there is evidence that the payment was passed from one Merchant to the other (for example: payment from a travel agent to a T&E Merchant)	**All**

ID# 0030304   Edition: Apr 2020 | Last Updated: Apr 2018

11.9.6.4   Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 12.6: Duplicate Processing/Paid by Other Means according to the following time limits:

Table 11-83: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Time Limit

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Dispute Time Limit	Country/Region
Either • 120 calendar days from the Transaction Processing Date • 120 calendar days from the Transaction date of a Shared Deposit Adjustment	**All**
120 calendar days from either: • The Transaction Processing Date • For an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit Transaction, the Transaction Date of the Adjustment	**US Domestic**

ID# 0030305   **Edition: Apr 2020 | Last Updated: Apr 2019**

11.9.6.5   Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 12.6: Duplicate Processing/Paid by Other Means:

Table 11-84: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Processing Requirements

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Supporting Documentation/Certification	Country/Region
For Duplicate Processing: • Certification of the date and Acquirer Reference Number of the valid Transaction • For a Shared Deposit Adjustment, certification of the first Adjustment date and amount For Transactions that were paid by other means all of the following, as applicable: • Certification that the Cardholder attempted to resolve the dispute with the Merchant, unless prohibited by applicable laws or regulations	**All**

Table 11-84: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Processing Requirements (continued)

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Supporting Documentation/Certification	Country/Region
• Evidence that the Merchant received payment by other means, including: – The Acquirer Reference Number or other Transaction information, if paid by a Visa Card – A statement, if paid by another card – A cash receipt – A copy of the front and back of a cancelled check • If the Merchant billed the Cardholder because the Merchant was unable to collect payment for a voucher received from a third party, evidence that the Merchant accepted the voucher for payment for the merchandise or service (for example: a rental contract showing that the voucher was accepted by the Merchant)	

ID# 0030306	Edition: Apr 2020 | Last Updated: Apr 2019

11.9.6.6   Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 12.6: Duplicate Processing/Paid by Other Means:

Table 11-85: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Response Processing Requirements

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • For an ATM Transaction, a copy of the ATM Cash Disbursement Transaction	**All**

Table 11-85: Dispute Condition 12.6: Duplicate Processing/Paid by Other Means – Dispute Response Processing Requirements (continued)

Dispute Condition 12.6: Duplicate Processing/Paid by Other Means Supporting Documentation/Certification	Country/Region
or Load Transaction records containing at least the following: – Payment Credential – Transaction time or sequential number that identifies individual Transactions – Indicator that confirms that the ATM Cash Disbursement or Load Transaction was successful • For a Transaction that is not an ATM Transaction, either: – 2 separate Transaction Receipts or other record to prove that separate Transactions were processed – Evidence to prove that the Merchant did not receive payment by other means for the same merchandise or service	

ID# 0030307	Edition: Apr 2020 | Last Updated: Apr 2020

11.9.7   Dispute Condition 12.7: Invalid Data

11.9.7.1   Dispute Condition 12.7: Invalid Data – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 12.7: Invalid Data for the following reason:

Table 11-86: Dispute Condition 12.7: Invalid Data – Dispute Reasons

Dispute Condition 12.7: Invalid Data Dispute Reasons	Country/Region
Either: • Authorization was obtained using invalid or incorrect data • The MCC used in the Authorization Request does not match the MCC in the Clearing Record of the first Presentment for the same Transaction.	All

ID# 0030308	Edition: Apr 2020 | Last Updated: Apr 2018

11.9.7.2   Dispute Condition 12.7: Invalid Data – Dispute Rights

Table 11-87: Dispute Condition 12.7 Invalid Data – Dispute Rights

Dispute Condition 12.7 Invalid Data Dispute Rights	Country/Region
• The Dispute applies for the entire Transaction amount. • The Authorization is invalid if the Authorization Request contained an incorrect Transaction Date, MCC, Merchant or Transaction type indicator, country code, state code, special condition indicator, or other required field.	**All**

ID# 0030309   Edition: Apr 2020 | Last Updated: Apr 2019

11.9.7.3   Dispute Condition 12.7: Invalid Data – Invalid Disputes

A Dispute is invalid under Dispute Condition 12.7: Invalid Data for the following:

Table 11-88: Dispute Condition 12.7: Invalid Data – Invalid Disputes

Dispute Condition 12.7: Invalid Data Invalid Disputes	Country/Region
• A Mobile Push Payment Transaction • **Effective for Disputes processed on or after 20 April 2020** An ATM Cash Disbursement	**All**

ID# 0030629   Edition: Apr 2020 | Last Updated: Apr 2020

11.9.7.4   Dispute Condition 12.7: Invalid Data – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 12.7: Invalid Data according to the following time limit:

Table 11-89: Dispute Condition 12.7: Invalid Data – Dispute Time Limit

Dispute Condition 12.7: Invalid Data Dispute Time Limit	Country/Region
75 calendar days from the Transaction Processing Date	**All**

ID# 0030310	Edition: Apr 2020 | Last Updated: Apr 2018

11.9.7.5   Dispute Condition 12.7: Invalid Data – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 12.7: Invalid Data:

Table 11-90: Dispute Condition 12.7: Invalid Data – Dispute Processing Requirements

Dispute Condition 12.7: Invalid Data Supporting Documentation/Certification	Country/Region
Both: • Certification that the Authorization Request would have been declined if valid data had been provided • An explanation of why the inclusion of valid data would have caused the Authorization Request to be declined	All

ID# 0030311	Edition: Apr 2020 | Last Updated: Apr 2018

11.9.7.6   Dispute Condition 12.7: Invalid Data – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 12.7 Invalid Data:

Table 11-91: Dispute Condition 12.7 Invalid Data – Dispute Response Processing Requirements

Dispute Condition 12.7 Invalid Data Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. • The Dispute is invalid. • The Cardholder no longer disputes the Transaction. • The Authorization did not contain invalid data.	All

ID# 0030312	Edition: Apr 2020 | Last Updated: Apr 2018

11.10   Dispute Category 13: Consumer Disputes

11.10.1   Dispute Category 13: Cardholder Letter Requirements

If the Dispute requires an Issuer to provide an Acquirer with a Cardholder[1] letter confirming non-receipt of merchandise, services, or Cash, the letter must be signed by the Cardholder[1] and include all of the following:

- Cardholder's[1] complete or partial Payment Credential
- Merchant name(s)
- Transaction amount(s)

[1] Or Virtual Account holder

ID# 0030224	Edition: Apr 2020 | Last Updated: Apr 2020

11.10.2   Dispute Condition 13.1: Merchandise/Services Not Received

11.10.2.1 Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.1: Merchandise/Services Not Received for the following reason:

Table 11-92: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Reasons

Dispute Condition 13.1: Merchandise/Services Not Received Dispute Reasons	Country/Region
The Cardholder[1] participated in the Transaction but the Cardholder[1] or an authorized person did not receive the merchandise or services because the Merchant or Prepaid Partner was unwilling or unable to provide the merchandise or services.	**All**
[1] Or Virtual Account holder	

ID# 0030313	Edition: Apr 2020 | Last Updated: Oct 2018

11.10.2.2   Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Rights

Table 11-93: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Rights

Dispute Condition 13.1: Merchandise/Services Not Received Dispute Rights	Country/Region
• The Dispute amount is limited to the portion of services or merchandise not received. • Before the Issuer may initiate a Dispute, the Cardholder must attempt to resolve the dispute with the Merchant or the Merchant's liquidator, if applicable.[1] • The Merchant is responsible for merchandise held in a customs agency in the Merchant's country. • If merchandise was delivered late or to the incorrect location, the Cardholder must return or attempt to return the merchandise.	**All**
• For a Dispute related to non-receipt of travel services from a provider who has failed, if the services are covered by a bonding authority/insurance scheme, the Issuer must attempt to obtain reimbursement from the relevant bonding authority/insurance scheme., unless the bond or insurance scheme is insufficient. If the bond or insurance scheme is insufficient, the Issuer may use information in the public domain to initiate the Dispute.	**Europe**
• Only applies if the Merchant is put into liquidation or receivership	**France Domestic**
[1] Does not apply to a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services	

ID# 0030314   Edition: Apr 2020 | Last Updated: Oct 2018

11.10.2.3   Dispute Condition 13.1: Merchandise/Services Not Received – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.1: Merchandise/Services Not Received for any of the following:

Table 11-94: Dispute Condition 13.1: Merchandise/Services Not Received – Invalid Disputes

Dispute Condition 13.1: Merchandise/Services Not Received Invalid Disputes	Country/Region
- An ATM Cash Disbursement - A Straight Through Processing Transaction - A Transaction in which the Cardholder cancelled the merchandise or service before the expected delivery or service date - A Transaction in which merchandise is being held by the Cardholder's country's customs agency - A Transaction that the Cardholder states is fraudulent - A dispute regarding the quality of merchandise or service provided - A partial Advance Payment[1] Transaction when the remaining balance was not paid and the Merchant is willing and able to provide the merchandise or services - The Cash-Back portion of a Visa Cash-Back Transaction	**All**
An Automated Fuel Dispenser Transaction	**All excluding Europe**
[1] Processed as specified in *Section 5.9.10.1, Requirements for Partial Payments, Advance Payments, and Transactions Using Stored Credentials*	

ID# 0030315	**Edition: Apr 2020	Last Updated: Apr 2020**

11.10.2.4   Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.1: Merchandise/Services Not Received according to the following time limits:

Table 11-95: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Time Limit

Dispute Condition 13.1: Merchandise/Services Not Received Dispute Time Limit	Country/Region
If applicable, before initiating a Dispute, an Issuer must wait 15 calendar days[1] from either: The Transaction Date, if the date the services were expected or the delivery	**All**

Table 11-95: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Time Limit (continued)

Dispute Condition 13.1: Merchandise/Services Not Received Dispute Time Limit	Country/Region
date for the merchandise is not specified • The date the Cardholder returned or attempted to return the merchandise, if the merchandise was returned due to late delivery A Dispute must be processed no later than either: • 120 calendar days from the Transaction Processing Date • 120 calendar days from the last date that the Cardholder expected to receive the merchandise or services[2]	

If applicable, before initiating a Dispute, an Issuer must either:
 	
• Wait 15 calendar days[1] from either:
 	
    • The Transaction Date, if the date the services were expected or the delivery date for the merchandise is not specified
 	
    • The date the Cardholder returned or attempted to return the merchandise, if the merchandise was returned due to late delivery
 	
• **Effective for Disputes processed on or after 20 April 2020** If the Issuer was required to attempt to obtain reimbursement from a bonding authority/insurance scheme, wait 60 calendar days from the date the claim was submitted to the bonding authority/insurance scheme before initiating a Dispute[1,3,4]
 	
A Dispute must be processed no later than any of the following:
 	
• 120 calendar days from the Transaction Processing Date
 	
• 120 calendar days from the last date that the Cardholder expected to receive the merchandise or services[2]
 	
• If the Issuer was required to attempt to obtain reimbursement from a bonding authority/insurance scheme, a Dispute must be processed no later than 60 days from the date of the letter or advice from the bonding authority/insurance scheme[2]
	Europe

[1] This does not apply if the waiting period would cause the Dispute to exceed the Dispute time limit.

[2] Not to exceed 540 calendar days from the Transaction Processing Date

[3] **Effective for Disputes processed on or after 20 April 2020** The waiting period does not apply if the bond or insurance scheme is insufficient.

Table 11-95: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Time Limit (continued)

Dispute Condition 13.1: Merchandise/Services Not Received Dispute Time Limit	Country/Region
[4] **Effective for Disputes processed on or after 20 April 2020** If no response is received from the bonding authority or insurance scheme within 60 calendar days, the Issuer may pursue the Dispute.	

ID# 0030316	Edition: Apr 2020 | Last Updated: Apr 2020

11.10.2.5   Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.1: Merchandise/Services Not Received:

Table 11-96: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Processing Requirements

Dispute Condition 13.1: Merchandise/Services Not Received Supporting Documentation/Certification	Country/Region

All of the following, as applicable:
 	
• Certification of any of the following, as applicable:
  – Services were not rendered by the expected date/time
  – Merchandise was not received by the expected date/time
  – Merchandise was not received at the agreed location (Issuer must specify the address of the agreed location)
  – Cardholder attempted to resolve with Merchant
  – The date the merchandise was returned
• A detailed description of the merchandise or services purchased, unless prohibited by applicable laws or regulations. This description must contain additional information beyond the data required in the Clearing Record.
• A Cardholder letter,[1] if both:
  – The Cardholder has disputed 3 or more Transactions for non-receipt of merchandise or services at the same Merchant on the same Card.
  – The disputed Transactions all occurred within the same 30-calendar day period.
	All

Table 11-96: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Processing Requirements (continued)

Dispute Condition 13.1: Merchandise/Services Not Received Supporting Documentation/Certification	Country/Region

All of the following, as applicable:
 	
• Certification of any of the following, as applicable:
 	
  – Services were not rendered by the expected date/time
 	
  – Merchandise was not received by the expected date/time
 	
  – Merchandise was not received at the agreed location (Issuer must specify the address of the agreed location)
 	
  – Cardholder attempted to resolve with Merchant
 	
  – The date the merchandise was returned
 	
• A detailed description of the merchandise or services purchased, unless prohibited by applicable laws or regulations. This description must contain additional information beyond the data required in the Clearing Record.
 	
• A Cardholder letter, if both:
 	
  – The Cardholder has disputed 3 or more Transactions for non-receipt of merchandise or services at the same Merchant on the same Card[1].
 	
  – The disputed Transactions all occurred within the same 30-calendar day period.
 	
• Unless prohibited by applicable laws or regulations, all of the following:
 	
  – The date the request for reimbursement was submitted to the bonding authority/insurance scheme
 	
  – An explanation of the attempt to resolve the dispute with the bonding authority/insurance scheme
 	
  – The date of the letter or advice from the bonding authority/insurance scheme
	Europe

[1] In the LAC Region (Brazil): For a domestic Installment Transaction, the 3 or more Dispute limit is calculated from the date of the original Authorization Request.	

11.10.2.6   Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.1: Merchandise/Services Not Received:

Table 11-97: Dispute Condition 13.1: Merchandise/Services Not Received – Dispute Response Processing Requirements

Dispute Condition 13.1: Merchandise/Services Not Received Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • Documentation to prove that the Cardholder or an authorized person received the merchandise or services at the agreed location or by the agreed date/time • For an Airline Transaction, evidence showing that the name is included in the manifest for the departed flight and it matches the name provided on the purchased itinerary • Compelling Evidence	**All**

ID# 0030318   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.10.3   Dispute Condition 13.2: Cancelled Recurring Transaction

11.10.3.1   Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.2: Cancelled Recurring Transaction for the following reasons:

Table 11-98: Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Reasons

Dispute Condition 13.2: Cancelled Recurring Transaction Dispute Reasons	Country/Region
Either: • The Cardholder withdrew permission to charge the account for a Recurring Transaction or, in the Europe Region, an Installment Transaction. • The Acquirer or Merchant received notification that, before the Transaction was processed, the Cardholder's account was closed or, in the Europe Region, facilities were withdrawn or the Cardholder deceased.	**All**

ID# 0030319 | **Edition: Apr 2020 | Last Updated: Apr 2018**

11.10.3.2   Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Rights

Table 11-99: Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Rights

Dispute Condition 13.2: Cancelled Recurring Transaction Dispute Rights	Country/Region
The Dispute amount is limited to the unused portion of the service or merchandise.[1]	**All**
[1] In the Europe Region: This does not apply to an Installment Transaction.	

ID# 0030320 | **Edition: Apr 2020 | Last Updated: Apr 2018**

11.10.3.3   Dispute Condition 13.2: Cancelled Recurring Transaction – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.2: Cancelled Recurring Transaction for the following:

Table 11-100: Dispute Condition 13.2: Cancelled Recurring Transaction – Invalid Disputes

Dispute Condition 13.2: Cancelled Recurring Transaction Invalid Disputes	Country/Region
• A Mobile Push Payment Transaction • A Straight Through Processing Transaction	**All**

Table 11-100: Dispute Condition 13.2: Cancelled Recurring Transaction – Invalid Disputes (continued)

Dispute Condition 13.2: Cancelled Recurring Transaction Invalid Disputes	Country/Region
• An Installment Transaction[1] • An Unscheduled Credential-on-File Transaction	
[1] In the Europe Region: This does not apply.	

ID# 0030321	Edition: Apr 2020 | Last Updated: Apr 2019

11.10.3.4   Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.2: Cancelled Recurring Transaction according to the following time limit:

Table 11-101: Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Time Limit

Dispute Condition 13.2: Cancelled Recurring Transaction Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**

ID# 0030322	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.3.5   Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.2: Cancelled Recurring Transaction:

Table 11-102: Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Processing Requirements

Dispute Condition 13.2: Cancelled Recurring Transaction Supporting Documentation/Certification	Country/Region
Certification of either: • The date the service was cancelled	**All**

Table 11-102: Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Processing Requirements (continued)

Dispute Condition 13.2: Cancelled Recurring Transaction Supporting Documentation/Certification	Country/Region
• The date the Merchant was notified that the account was closed	
Certification of any of the following: • The date the service was cancelled • The date the Merchant was notified that the account was closed • The account was closed and facilities were withdrawn • Cardholder deceased	**Europe**

ID# 0030323   Edition: Apr 2020 | Last Updated: Apr 2018

11.10.3.6   Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.2: Cancelled Recurring Transaction:

Table 11-103: Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Response Processing Requirements

Dispute Condition 13.2: Cancelled Recurring Transaction Supporting Documentation/Certification	Country/Region
Evidence of one or more of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • The Cardholder requested cancellation for a different date and services were provided until this date[1] • The Merchant posts charges to Cardholders after services have been provided and that the Cardholder received services until the cancellation date[1]	**All**

Table 11-103: Dispute Condition 13.2: Cancelled Recurring Transaction – Dispute Response Processing Requirements (continued)

Dispute Condition 13.2: Cancelled Recurring Transaction Supporting Documentation/Certification	Country/Region
• The Issuer's claim is invalid that the Acquirer or Merchant was notified that the account was closed[1]	
[1] In the Europe Region: This does not apply when the Issuer has advised that the account was closed, facilities withdrawn, or Cardholder deceased	

ID# 0030324	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.4   Dispute Condition 13.3: Not as Described or Defective Merchandise/Services

11.10.4.1   Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.3: Not as Described or Defective Merchandise/Services for the following reasons:

Table 11-104: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Reasons

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Dispute Reasons	Country/Region
One of the following: • The merchandise or services did not match what was described on the Transaction Receipt or other record presented at the time of purchase. • The merchandise received by the Cardholder was damaged or defective. • The Cardholder disputes the quality of the merchandise or services received. • For a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services, either: – The Merchant failed to honor the contractual agreement. – The services provided by the Merchant to the Virtual Account holder were not as described in the contractual agreement.	**All excluding France Domestic**
For a Card-Absent Environment Transaction, the Merchant's verbal description	**Canada Domestic**

Table 11-104: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Reasons (continued)

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Dispute Reasons	Country/Region
or other documentation presented at the time of purchase did not match the merchandise or services received.	**US Domestic** **Canada/US Interregional**

ID# 0030325	Edition: Apr 2020 | Last Updated: Oct 2018

11.10.4.2   Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Rights

Table 11-105: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Rights

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Dispute Rights	Country/Region

• The Dispute amount is limited to one of the following:
   – The unused portion of the cancelled service
   – The value of the merchandise that the Cardholder returned or, if applicable, attempted to return
   – For a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services, the value of any items not listed in the contractual agreement
 • Before the Issuer may initiate a Dispute, the Cardholder must attempt to resolve the dispute with the Merchant or the Merchant's liquidator.[1]
 • The Merchant is responsible for merchandise held in a customs agency in the Merchant's country.
	All

Before the Issuer may initiate a Dispute, the Cardholder must return or attempt to return the merchandise or cancel the services.[1,2]	**All excluding Europe**
Before the Issuer may initiate a Dispute, the Cardholder must return the merchandise or cancel the services.[1,2] If the Cardholder is unable to return merchandise that was delivered or installed by the Merchant, it is sufficient for the Cardholder to attempt to return the merchandise.[1]	**Europe and Interregional including Europe**

Table 11-105: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Rights (continued)

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Dispute Rights	Country/Region
[1] Does not apply to a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services [2] For Disputes related to services that cannot be cancelled, the Cardholder must request a credit from the Merchant.	

ID# 0030326   **Edition: Apr 2020 | Last Updated: Oct 2018**

11.10.4.3   Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.3: Not as Described or Defective Merchandise/Services for any of the following:

Table 11-106: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Invalid Disputes

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Invalid Disputes	Country/Region
• An ATM Cash Disbursement • A Straight Through Processing Transaction • A dispute regarding Value-Added Tax (VAT) • A Transaction in which the returned merchandise is held by any customs agency except the Merchant's country's customs agency • The Cash-Back portion of a Visa Cash-Back Transaction	**All**

ID# 0030327   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.10.4.4   Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.3: Not as Described or Defective Merchandise/Services according to the following time limits:

Table 11-107: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Time Limit

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Dispute Time Limit	Country/Region

Before initiating a Dispute, the Issuer must wait 15 calendar days[1,2] from the date the Cardholder returned or attempted to return the merchandise or cancelled the services.
 	
A Dispute must be processed within either:
 	
• 120 calendar days of either:
 	
  – The Transaction Processing Date
 	
  – The date the Cardholder[3] received the merchandise or services[4]
 	
• 60 calendar days of the date the Issuer received the first Cardholder notification of the dispute, if both:[4]
 	
  – There is evidence in the notification of previous ongoing negotiations between the Cardholder and the Merchant to resolve the dispute.
 	
  – The negotiations occurred within 120 days of the Transaction Processing Date.
	All

[1] This does not apply if the waiting period would cause the Dispute to exceed the Dispute time limit or if the Merchant refuses the cancellation or return. [2] The waiting period does not apply to a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services [3] Or Virtual Account holders [4] Not to exceed 540 calendar days from the Transaction Processing Date	

ID# 0030328   Edition: Apr 2020 | Last Updated: Apr 2020

11.10.4.5   Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.3: Not as Described or Defective Merchandise/Services:

Table 11-108: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Processing Requirements

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Supporting Documentation/Certification	Country/Region

Certification of the following, as applicable:
 	
• An explanation of what was not as described or defective or information regarding the quality-related issue
 	
• The date the Cardholder received the merchandise or services
 	
• That the Cardholder attempted to resolve the dispute with the Merchant
 	
• For services, the date the Cardholder cancelled the services or requested a credit from the Merchant
 	
• For merchandise, the date the Cardholder returned or attempted to return the merchandise
 	
• For merchandise that the Cardholder returned, all of the following:
 	
  – The name of the shipping company
 	
  – A tracking number (if available)
 	
  – The date the Merchant received the merchandise
 	
• For merchandise that the Cardholder attempted to return, all of the following:
 	
  – A detailed explanation of how and when the Cardholder attempted to return the merchandise
 	
  – The disposition of the merchandise
 	
  – Certification that the Merchant either:
 	
    ▪ Refused the return of the merchandise
 	
    ▪ Refused to provide a return merchandise authorization
 	
    ▪ Instructed the Cardholder not to return the merchandise
 	
• For a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services, an explanation on how the terms of service included in the contractual agreement were not as described or not honored by the Merchant.
 	
• For disputes involving ongoing negotiations, all of the following:
	All

Table 11-108: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Processing Requirements (continued)

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Supporting Documentation/Certification	Country/Region

– Certification of both:
 	
  ▪ The date the Cardholder began negotiations with the Merchant
 	
  ▪ The date the Issuer was first notified of the dispute
 	
– Evidence of ongoing negotiations between the Cardholder and the Merchant to resolve the dispute	

ID# 0030329   Edition: Apr 2020 | Last Updated: Apr 2019

11.10.4.6   Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.3: Not as Described or Defective Merchandise/Services:

Table 11-109: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Response Processing Requirements

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Supporting Documentation/Certification	Country/Region

Either:
 	
• Evidence that one of the following:
 	
  – A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute.
 	
  – The Dispute is invalid.
 	
  – The Cardholder no longer disputes the Transaction.
 	
• All of the following:
 	
  – Evidence to prove that the merchandise or service matched what was described (including the description of the quality of the merchandise or service) or was not damaged or defective
 	
  – Merchant rebuttal to the Cardholder's claims
	All

Table 11-109: Dispute Condition 13.3: Not as Described or Defective Merchandise/Services – Dispute Response Processing Requirements (continued)

Dispute Condition 13.3: Not as Described or Defective Merchandise/Services Supporting Documentation/Certification	Country/Region
– If applicable, evidence to prove that the Cardholder did not attempt to return the merchandise or certification that the returned merchandise has not been received • For a Dispute where a travel agency using a Visa Commercial Card Virtual Account has a contractual agreement with a Lodging Merchant or Vehicle Rental Merchant that covers the terms for specified services, evidence to prove that the terms of service included in the contractual agreement were as described or honored by the Merchant	

ID# 0030330	Edition: Apr 2020 | Last Updated: Oct 2018

11.10.5   Dispute Condition 13.4: Counterfeit Merchandise

11.10.5.1   Dispute Condition 13.4: Counterfeit Merchandise – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.4: Counterfeit Merchandise for the following reasons:

Table 11-110: Dispute Condition 13.4: Counterfeit Merchandise – Dispute Reasons

Dispute Condition 13.4: Counterfeit Merchandise Dispute Reasons	Country/Region
The merchandise was identified as counterfeit by one or more of the following: • The owner of the intellectual property or its authorized representative • A customs agency, law enforcement agency, or other government agency • A third-party expert	**All excluding France Domestic**

ID# 0030331	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.5.2   Dispute Condition 13.4: Counterfeit Merchandise – Dispute Rights

Table 11-111: Dispute Condition 13.4: Counterfeit Merchandise – Dispute Rights

Dispute Condition 13.4: Counterfeit Merchandise Dispute Rights	Country/Region
If the Cardholder was advised that the merchandise ordered was counterfeit, the Dispute applies even if the Cardholder has not received the merchandise.	**All**

ID# 0030332	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.5.3   Dispute Condition 13.4: Counterfeit Merchandise – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.4: Counterfeit Merchandise for any of the following:

Table 11-112: Dispute Condition 13.4: Counterfeit Merchandise – Invalid Disputes

Dispute Condition 13.4: Counterfeit Merchandise Invalid Disputes	Country/Region
• A Straight Through Processing Transaction • A dispute regarding Value-Added Tax (VAT) • The Cash-Back portion of a Visa Cash-Back Transaction	**All**

ID# 0030333	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.5.4   Dispute Condition 13.4: Counterfeit Merchandise – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.4: Counterfeit Merchandise according to the following time limits:

Table 11-113: Dispute Condition 13.4: Counterfeit Merchandise – Dispute Time Limit

Dispute Condition 13.4: Counterfeit Merchandise Dispute Time Limit	Country/Region
A Dispute must be processed no later than 120 calendar days from one of the following: • The Transaction Processing Date	**All**

Table 11-113: Dispute Condition 13.4: Counterfeit Merchandise – Dispute Time Limit (continued)

Dispute Condition 13.4: Counterfeit Merchandise Dispute Time Limit	Country/Region
• The date the Cardholder received the merchandise[1] • The date on which the Cardholder was notified that the merchandise was counterfeit[1]	
[1] Not to exceed 540 calendar days from the Transaction Processing Date	

11.10.5.5   Dispute Condition 13.4: Counterfeit Merchandise – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.4: Counterfeit Merchandise:

Table 11-114: Dispute Condition 13.4: Counterfeit Merchandise – Dispute Processing Requirements

Dispute Condition 13.4: Counterfeit Merchandise Supporting Documentation/Certification	Country/Region
Certification of all of the following: • That the Cardholder received notification from one of the entities listed in *Section 11.10.5.1, Dispute Condition 13.4: Counterfeit Merchandise – Dispute Reasons,* that the merchandise is counterfeit • The date the Cardholder received the merchandise or received notification that the merchandise was counterfeit • A description of the counterfeit merchandise • The disposition of the merchandise • Information about the entity that indicated the merchandise to be counterfeit, including the name of the entity providing the notification and validation that the entity is qualified to provide the notification	**All**

11.10.5.6   Dispute Condition 13.4: Counterfeit Merchandise – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.4: Counterfeit Merchandise:

Table 11-115: Dispute Condition 13.4: Counterfeit Merchandise – Dispute Response Processing Requirements

Dispute Condition 13.4: Counterfeit Merchandise Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • To support the Merchant's claim that the merchandise was not counterfeit	**All**

ID# 0030336   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.10.6   Dispute Condition 13.5: Misrepresentation

11.10.6.1   Dispute Condition 13.5: Misrepresentation – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.5: Misrepresentation for the following reason:

Table 11-116: Dispute Condition 13.5: Misrepresentation – Dispute Reasons

Dispute Condition 13.5: Misrepresentation Dispute Reasons	Country/Region
The Cardholder claims that the terms of sale were misrepresented by the Merchant.	**All excluding France Domestic**

ID# 0030337   **Edition: Apr 2020 | Last Updated: Oct 2019**

11.10.6.2   Dispute Condition 13.5: Misrepresentation – Dispute Rights

Table 11-117: Dispute Condition 13.5: Misrepresentation – Dispute Rights

Dispute Condition 13.5: Misrepresentation Dispute Rights	Country/Region
• The Dispute amount is limited to the unused portion of the cancelled service or value of the merchandise that the Cardholder returned or, if applicable, attempted to return. • Before the Issuer may initiate a Dispute, the Cardholder must attempt to resolve the dispute with the Merchant or the Merchant's liquidator. • The Merchant is responsible for merchandise held in a customs agency in the Merchant's country.	**All**

The Dispute applies for any of the following:
 	
• A Transaction at a Merchant that is a timeshare reseller, a timeshare reseller advertiser, or that recovers timeshare reseller fees[1]
 	
• A Card-Absent Environment Transaction at a Merchant that represents that it recovers, consolidates, reduces, or amends existing financial products or services, including:[2]
 	
  – Debt consolidation
 	
  – Credit repair/counseling
 	
  – Mortgage repair/modification/counseling
 	
  – Foreclosure relief services
 	
  – Credit card interest rate reduction services
 	
• Technical services, technical support, or computer software that is sold using inaccurate online advertisements or that contains malicious software downloads.
 	
• Business opportunities in which the Merchant suggests that an income will be generated or recommends that the Cardholder purchases additional items (such as better sales leads) to generate more income
 	
• A Transaction in which a Merchant advises the Cardholder that the Merchant can recover the Cardholder's funds and fails to provide services
 	
• A Transaction at an outbound telemarketing Merchant
 	
• Investment products or services (for example: binary options or foreign exchange trading), where the Merchant refuses to allow the Cardholder to
	All excluding Europe

Table 11-117: Dispute Condition 13.5: Misrepresentation – Dispute Rights (continued)

Dispute Condition 13.5: Misrepresentation Dispute Rights	Country/Region
withdraw available balances	

The Dispute applies for any of the following:
 	
• A Transaction at a Merchant that is a timeshare reseller, a timeshare reseller advertiser, or that recovers timeshare reseller fees[1]
 	
• A Card-Absent Environment Transaction at a Merchant that sells the following merchandise or services:
 	
  – The recovery, consolidation, reduction, or amendment of existing financial products or services[2]
 	
  – Technical services, technical support, or computer software that is sold using inaccurate online advertisements or that contains malicious software downloads.
 	
  – Business opportunities in which the Merchant suggests that an income will be generated or recommends that the Cardholder purchases additional items (such as better sales leads) to generate more income
 	
• Investment products or services (for example: binary options or foreign exchange trading), where the Merchant refuses to allow the Cardholder to withdraw available balances
	Europe and Interregional including Europe

Effective for Disputes processed through 17 April 2020 The Dispute applies for Transactions that take place in a Card-Absent Environment where merchandise has been purchased through a trial period, or, as a one-off purchase and the Cardholder was not clearly advised of further billing after the purchase date.	**Europe**
Effective for Disputes processed on or after 18 April 2020 The Dispute applies for a Transaction in a Card-Absent Environment where merchandise or digital goods have been purchased through a trial period, promotional period, or introductory offer or as a one-off purchase and the Cardholder was not clearly advised of further Transactions after the purchase date.	**All**

[1] This applies only to a Merchant that offers reseller services that are connected to timeshare property it does not own.

[2] This condition is based on the type of merchandise or services sold and not solely on the MCC.

ID# 0030338   **Edition: Apr 2020 | Last Updated: Oct 2019**

11.10.6.3   Dispute Condition 13.5: Misrepresentation – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.5: Misrepresentation for any of the following:

Table 11-118: Dispute Condition 13.5: Misrepresentation – Invalid Disputes

Dispute Condition 13.5: Misrepresentation Invalid Disputes	Country/Region
• A Straight Through Processing Transaction • A dispute regarding Value-Added Tax (VAT) • A dispute related solely to the quality of merchandise or services provided • The Cash-Back portion of a Visa Cash-Back Transaction	**All**

ID# 0030339	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.6.4   Dispute Condition 13.5: Misrepresentation – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.5: Misrepresentation according to the following time limits:

Table 11-119: Dispute Condition 13.5: Misrepresentation – Dispute Time Limit

Dispute Condition 13.5: Misrepresentation Dispute Time Limit	Country/Region

A Dispute must be processed within either:
 	
• 120 calendar days of either:
 	
  – The Transaction Processing Date
 	
  – The date the Cardholder received the merchandise or services[1]
 	
• 60 calendar days of the date the Issuer received the first Cardholder notification of the dispute, if both:[1]
 	
  – There is evidence in the notification of previous ongoing negotiations between the Cardholder and the Merchant to resolve the dispute.
 	
  – The negotiations occurred within 120 days of the Transaction Processing Date.
	All

[1] The Dispute Processing Date must be no later than 540 calendar days from the Transaction Processing Date.	

ID# 0030340	Edition: Apr 2020 Last Updated: Apr 2020

11.10.6.5   Dispute Condition 13.5: Misrepresentation – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.5: Misrepresentation:

Table 11-120: Dispute Condition 13.5: Misrepresentation – Dispute Processing Requirements

Dispute Condition 13.5: Misrepresentation Supporting Documentation/Certification	Country/Region

All of the following:
 	
• Certification of all of the following, as applicable:
  – The date the merchandise was returned or the service was cancelled
  – The name of the shipping company
  – The invoice/tracking number (if available)
  – The date the Merchant received the merchandise
  – Certification that the Merchant refused the return of merchandise, refused to provide a return merchandise authorization, or informed the Cardholder not to return the merchandise
  – That the Cardholder attempted to resolve the dispute with the Merchant
  – An explanation of what was not as described or defective
  – The date the Cardholder received the merchandise or services
 	
• An explanation of how the Merchant's verbal and/or written representations do not match the terms of sale to which the Cardholder agreed
 	
• Copy of the Cardholder's investment account showing the date, withdrawal amount, and available balance at the time the withdrawal request was made
 	
• For Disputes involving ongoing negotiations, both:
  – Certification of both:
    ▪ The date the Cardholder began negotiations with the Merchant
    ▪ The date the Issuer was first notified of the dispute
  – Evidence of ongoing negotiations between the Cardholder and the Merchant to resolve the Dispute
	Effective for Disputes processed through 17 April 2020
	All excluding Europe
	
	Effective for Disputes processed on or after 18 April 2020
	All

Table 11-120: Dispute Condition 13.5: Misrepresentation – Dispute Processing Requirements (continued)

Dispute Condition 13.5: Misrepresentation Supporting Documentation/Certification	Country/Region

Effective for Disputes processed through 17 April 2020
 	
All of the following
 	
- Certification of all of the following, as applicable:
  – The date the merchandise was returned or the service was cancelled
  – The name of the shipping company
  – The invoice/tracking number (if available)
  – The date the Merchant received the merchandise
  – Certification that the Merchant refused the return of merchandise, refused to provide a return merchandise authorization, or informed the Cardholder not to return the merchandise
  – That the Cardholder attempted to resolve the dispute with the Merchant
  – The date the Cardholder received the merchandise or services
- Evidence from the Cardholder describing how the Merchant's written representations do not match the terms of sale to which the Cardholder agreed
- Copy of the Cardholder's investment account showing the date, withdrawal amount, and available balance at the time the withdrawal request was made
- For Disputes involving ongoing negotiations, both:
  – Certification of both:
    ▪ The date the Cardholder began negotiations with the Merchant
    ▪ The date the Issuer was first notified of the dispute
  – Evidence of ongoing negotiations between the Cardholder and the Merchant to resolve the Dispute
	Europe and Interregional including Europe

ID# 0030341   Edition: Apr 2020 | Last Updated: Apr 2020

11.10.6.6   Dispute Condition 13.5: Misrepresentation – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.5: Misrepresentation:

Table 11-121: Dispute Condition 13.5: Misrepresentation – Dispute Response Processing Requirements

Dispute Condition 13.5: Misrepresentation Supporting Documentation/Certification	Country/Region

Evidence of one of the following:
 	
• A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute
 	
• The Dispute is invalid
 	
• The Cardholder no longer disputes the Transaction
 	
• To prove that the terms of sale were not misrepresented
 	
• **Effective for Disputes processed on or after 18 April 2020** For a Dispute relating to a Transaction in a Card-Absent Environment where merchandise or digital goods have been purchased through a trial period, promotional period, or introductory offer or as a one-off purchase, both:
 	
  – To prove that, at the time of the initial Transaction, the Cardholder expressly agreed to future Transactions
 	
  – To prove that the Merchant notified the Cardholder of future Transactions at least 7 days before the Transaction Date
	All

ID# 0030342

Edition: Apr 2020 | Last Updated: Oct 2019

11.10.7   Dispute Condition 13.6: Credit Not Processed

11.10.7.1   Dispute Condition 13.6: Credit Not Processed – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.6: Credit Not Processed for the following reason:

Table 11-122: Dispute Condition 13.6: Credit Not Processed – Dispute Reasons

Dispute Condition 13.6: Credit Not Processed Dispute Reasons	Country/Region
Either: • The Cardholder received a credit or voided Transaction Receipt that was not processed. • For an ATM Transaction, the Cardholder disputes the validity of the Adjustment, including a Shared Deposit Adjustment, because the original Transaction was either cancelled or reversed.	**All**

ID# 0030343	Edition: Apr 2020 | Last Updated: Apr 2019

11.10.7.2   Dispute Condition 13.6: Credit Not Processed – Dispute Rights

Table 11-123: Dispute Condition 13.6: Credit Not Processed – Dispute Rights

Dispute Condition 13.6: Credit Not Processed Dispute Rights	Country/Region
The Dispute applies if a "void" or "cancelled" notation appears on the Transaction Receipt.	**All**

ID# 0030344	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.7.3   Dispute Condition 13.6: Credit Not Processed – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.6: Credit Not Processed for any of the following:

Table 11-124: Dispute Condition 13.6: Credit Not Processed – Invalid Disputes

Dispute Condition 13.6: Credit Not Processed Invalid Disputes	Country/Region
• An ATM Cash Disbursement • A Mobile Push Payment Transaction • A Straight Through Processing Transaction • The Cash-Back portion of a Visa Cash-Back Transaction	**All**

Table 11-124: Dispute Condition 13.6: Credit Not Processed – Invalid Disputes (continued)

Dispute Condition 13.6: Credit Not Processed Invalid Disputes	Country/Region
• A dispute regarding Value-Added Tax (VAT), unless a Credit Transaction Receipt is provided	
An Automated Fuel Dispenser Transaction	**All excluding Europe**

ID# 0030345   Edition: Apr 2020 | Last Updated: Apr 2019

11.10.7.4   Dispute Condition 13.6: Credit Not Processed – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.6: Credit Not Processed according to the following time limits:

Table 11-125: Dispute Condition 13.6: Credit Not Processed – Dispute Time Limit

Dispute Condition 13.6: Credit Not Processed Dispute Time Limit	Country/Region
Before initiating a Dispute, an Issuer must wait 15 calendar days[1] from the date on the Credit Transaction Receipt. This requirement does not apply if the Credit Transaction Receipt is undated. A Dispute must be processed no later than 120 calendar days from either: • The Transaction Processing Date • The date on the Credit Transaction Receipt[2] For an ATM Transaction, a Dispute must be processed no later than 120 calendar days from the Transaction Processing Date of the Adjustment, including a Shared Deposit Adjustment.	**All**
[1] This does not apply if the waiting period would cause the Dispute to exceed the Dispute time limit or if the Merchant refuses the cancellation or return.	
[2] If the Credit Transaction Receipt is undated, the date the Cardholder cancelled services or returned the merchandise	

ID# 0030346   Edition: Apr 2020 | Last Updated: Apr 2020

11.10.7.5   Dispute Condition 13.6: Credit Not Processed – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.6: Credit Not Processed:

Table 11-126: Dispute Condition 13.6: Credit Not Processed – Dispute Processing Requirements

Dispute Condition 13.6: Credit Not Processed Supporting Documentation/Certification	Country/Region
A copy of the Credit Transaction Receipt or voided Transaction Receipt	**All**

ID# 0030347   Edition: Apr 2020 | Last Updated: Apr 2018

11.10.7.6   Dispute Condition 13.6: Credit Not Processed – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.6: Credit Not Processed:

Table 11-127: Dispute Condition 13.6: Credit Not Processed – Dispute Response Processing Requirements

Dispute Condition 13.6: Credit Not Processed Supporting Documentation/Certification	Country/Region
Evidence that one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute. • The Dispute is invalid. • The Cardholder no longer disputes the Transaction.	**All**

ID# 0030348   Edition: Apr 2020 | Last Updated: Apr 2018

11.10.8   Dispute Condition 13.7: Cancelled Merchandise/Services

11.10.8.1   Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.7: Cancelled Merchandise/Services for the following reason:

Table 11-128: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Reasons

Dispute Condition 13.7: Cancelled Merchandise/Services Dispute Reasons	Country/Region
All of the following: • The Cardholder cancelled or returned merchandise, cancelled services, cancelled a timeshare Transaction, or cancelled a Guaranteed Reservation.[1] • The Merchant did not process a credit or voided Transaction Receipt. • Either: – The Merchant did not properly disclose or did disclose, but did not apply, a limited return or cancellation policy at the time of the Transaction. – In the Europe Region: The merchandise or services relate to an off-premises, distance selling contract (as set out in the EU Directive and amended from time to time) which is always subject to a 14-day cancellation period.	All
[1] In the Europe Region (France): For a Domestic Transaction, the Dispute is valid only for timeshare Transactions and No-Show Transactions.	

ID# 0030349   Edition: Apr 2020 | Last Updated: Apr 2018

11.10.8.2   Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Rights

Table 11-129: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Rights

Dispute Condition 13.7: Cancelled Merchandise/Services Dispute Rights	Country/Region
• If the merchandise was shipped before the Transaction was cancelled, the Cardholder must return the merchandise, if received. • The Dispute amount is limited to either:	All

Table 11-129: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Rights (continued)

Dispute Condition 13.7: Cancelled Merchandise/Services Dispute Rights	Country/Region
– The value of the unused portion of the cancelled service – The value of the returned merchandise • The Dispute applies if the returned merchandise is refused by the Merchant. • For a timeshare Transaction, either: – The Dispute applies for a timeshare Transaction processed with an incorrect MCC. – The Dispute applies if the Cardholder cancelled a timeshare Transaction within 14 calendar days of the contract date or the date the contract or related documents were received. If the Cardholder cancels a timeshare Transaction after 14 calendar days from the contract date or the date the contract or related documents were received, the Cardholder must cancel according to the Merchant's properly disclosed limited return or cancellation policy. • For a Guaranteed Reservation: – The Dispute applies if the Cardholder cancelled a Guaranteed Reservation with the Merchant or its agent according to the cancellation policy, but was billed for a No-Show Transaction. – The Dispute applies if the Merchant or its agent processed a No-Show Transaction for more than one day's accommodation or rental and applicable taxes when a Guaranteed Reservation was cancelled or unclaimed. – The Dispute applies if the Cardholder made a reservation and attempted to cancel within 24 hours of delivery of the reservation confirmation, but was billed for a No-Show Transaction. • Before the Issuer may initiate a Dispute, the Cardholder must attempt to resolve the dispute with the Merchant or the Merchant's liquidator. • The Merchant is responsible for merchandise held in a customs agency in the Merchant's country.	
• The Dispute applies if the Cardholder cancelled a Transaction related to an off-premises, distance selling contract (as set out in the EU Directive and amended from time to time) within 14 days. • The cancellation period for off-premises, distance selling does not apply to	**Europe**

Table 11-129: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Rights (continued)

Dispute Condition 13.7: Cancelled Merchandise/Services Dispute Rights	Country/Region
contracts for goods or services where any of the following apply: – Price is dependent on fluctuations in the financial market. – Made to measure goods are supplied. – Goods are liable to deteriorate or expire rapidly. – Sealed goods, subject to health and safety provisions, are supplied. – Goods are not received in physical form (software download). – The Transaction is a T&E Transaction. – The Merchant Outlet is based in Israel, Switzerland, or Turkey.	

ID# 0030350	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.8.3   Dispute Condition 13.7: Cancelled Merchandise/Services – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.7: Cancelled Merchandise/Services for any of the following:

Table 11-130: Dispute Condition 13.7: Cancelled Merchandise/Services – Invalid Disputes

Dispute Condition 13.7: Cancelled Merchandise/Services Invalid Disputes	Country/Region
• An ATM Cash Disbursement • A Straight Through Processing Transaction • A dispute regarding the quality of the service rendered or the quality of merchandise, unless a Credit Transaction Receipt is provided • A dispute regarding Value-Added Tax (VAT), unless a Credit Transaction Receipt is provided • A Transaction in which returned merchandise is held by a customs agency other than the Merchant's country's customs agency[1] • The Cash-Back portion of a Visa Cash-Back Transaction	**All**
• An Automated Fuel Dispenser Transaction	**All excluding Europe**

Table 11-130: Dispute Condition 13.7: Cancelled Merchandise/Services – Invalid Disputes (continued)

Dispute Condition 13.7: Cancelled Merchandise/Services Invalid Disputes	Country/Region
[1] In the Europe Region: This does not apply to an off-premises, distance selling Transaction.	

ID# 0030351   Edition: Apr 2020 | Last Updated: Oct 2019

11.10.8.4   Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.7: Cancelled Merchandise/Services according to the following time limits:

Table 11-131: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Time Limit

Dispute Condition 13.7: Cancelled Merchandise/Services Dispute Time Limit	Country/Region
Before initiating a Dispute, an Issuer must wait 15 calendar days[1] from the date the merchandise was returned. A Dispute must be processed no later than 120 calendar days from one of the following: • The Transaction Processing Date • The date the Cardholder received or expected to receive the merchandise or services, not to exceed 540 calendar days from the Transaction Processing Date • For an Adjustment of a PIN-Authenticated Visa Debit Transaction, the date of the Adjustment	**All**
[1] This does not apply if the waiting period would cause the Dispute to exceed the Dispute time limit.	

ID# 0030352   Edition: Apr 2020 | Last Updated: Apr 2018

11.10.8.5 Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.7: Cancelled Merchandise/Services:

Table 11-132: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Processing Requirements

Dispute Condition 13.7: Cancelled Merchandise/Services Supporting Documentation/Certification	Country/Region

Certification of the following, as applicable:
 	
• For a Timeshare Transaction, both:
  – The cancellation date
  – The date the contract was received by the Cardholder, if applicable
 	
• For a Guaranteed Reservation, the Merchant processed a No-Show Transaction, the date of the expected services, and one of the following:
  – **Effective for Disputes processed through 16 October 2020** The Cardholder properly cancelled the Guaranteed Reservation
  – **Effective for Disputes processed on or after 17 October 2020** The date the Cardholder properly cancelled the Guaranteed Reservation
  – The Cardholder attempted to cancel within 24 hours of delivery of the reservation confirmation
  – The Merchant billed a No-Show Transaction for more than one day's accommodation or rental
 	
• For all other Transactions, all of the following, as applicable:
  – The date the merchandise or service was expected or received
  – The date the merchandise or service was cancelled or returned
  – The name of the shipping company
  – The invoice/tracking number
  – The date the Merchant received the merchandise
  – For returned merchandise, that the Cardholder attempted to resolve the dispute with the Merchant
  – That the Merchant refused the return of merchandise, refused to provide a return merchandise authorization, or informed the Cardholder not to return the merchandise
	All

Table 11-132: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Processing Requirements (continued)

Dispute Condition 13.7: Cancelled Merchandise/Services Supporting Documentation/Certification	Country/Region

Certification of the following, as applicable:
 	
● For a Timeshare Transaction, both:
  – The cancellation date
  – The date the contract was received by the Cardholder, if applicable
 	
● For a Guaranteed Reservation, the Merchant processed a No-Show Transaction, the date of the expected services, and one of the following:
  – The Cardholder properly cancelled the Guaranteed Reservation
  – The Cardholder attempted to cancel within 24 hours of delivery of the reservation confirmation
  – The Merchant billed a No-Show Transaction for more than one day's accommodation or rental
 	
● For all other Transactions, all of the following, as applicable:
  – The date the merchandise or service was expected or received
  – The date the merchandise or service was cancelled or returned
  – The name of the shipping company
  – The invoice/tracking number
  – The date the Merchant received the merchandise
  – For returned merchandise, that the Cardholder attempted to resolve the dispute with the Merchant
  – That the Merchant refused the return of merchandise, refused to provide a return merchandise authorization, or informed the Cardholder not to return the merchandise
 	
For a Transaction related to off-premises, distance selling contracts, evidence of the following:
 	
● The start date of the off-premises, distance selling contract
● The Cardholder cancelled the Transaction within the 14-day cancellation period
	Europe

ID# 0030353	Edition: Apr 2020 | Last Updated: Apr 2020

11.10.8.6   Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.7: Cancelled Merchandise/Services:

Table 11-133: Dispute Condition 13.7: Cancelled Merchandise/Services – Dispute Response Processing Requirements

Dispute Condition 13.7: Cancelled Merchandise/Services Supporting Documentation/Certification	Country/Region
Evidence of one of the following: • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid • The Cardholder no longer disputes the Transaction • The Transaction Receipt or other record to prove that the Merchant properly disclosed a limited return or cancellation policy at the time of the Transaction • To demonstrate that the Cardholder received the Merchant's cancellation or return policy and did not cancel according to the disclosed policy	**All**

ID# 0030354	Edition: Apr 2020 | Last Updated: Apr 2018

11.10.9   Dispute Condition 13.8: Original Credit Transaction Not Accepted

11.10.9.1   Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.8: Original Credit Transaction Not Accepted for the following reason:

Table 11-134: Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Reasons

Dispute Condition 13.8: Original Credit Transaction Not Accepted Dispute Reasons	Country/Region
An Original Credit Transaction was not accepted because either: • The recipient refused the Original Credit Transaction. • Original Credit Transactions are prohibited by applicable laws or regulations.	**All**

ID# 0030355	**Edition: Apr 2020 | Last Updated: Apr 2018**

11.10.9.2   Dispute Condition 13.8 Original Credit Transaction Not Accepted – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.8: Original Credit Transaction Not Accepted for the following:

Table 11-135: Dispute Condition 13.8: Original Credit Transaction Not Accepted – Invalid Disputes

Dispute Condition 13.8: Original Credit Transaction Not Accepted Invalid Disputes	Country/Region
A Mobile Push Payment Transaction	**All**

ID# 0030553	**Edition: Apr 2020 | Last Updated: Apr 2019**

11.10.9.3   Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.8: Original Credit Transaction Not Accepted according to the following time limit:

Table 11-136: Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Time Limit

Dispute Condition 13.8: Original Credit Transaction Not Accepted Dispute Time Limit	Country/Region
120 calendar days from the Original Credit Transaction Processing Date	**All**

| ID# 0030357 | Edition: Apr 2020 | Last Updated: Apr 2018 |

11.10.9.4   Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.8: Original Credit Transaction Not Accepted:

Table 11-137: Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Processing Requirements

Dispute Condition 13.8: Original Credit Transaction Not Accepted Supporting Documentation/Certification	Country/Region
Certification that either: • An Original Credit Transaction is not allowed by applicable laws or regulations. • The recipient refused to accept the Original Credit Transaction.	All

---

| ID# 0030358 | Edition: Apr 2020 | Last Updated: Apr 2018 |

11.10.9.5   Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.8: Original Credit Transaction Not Accepted:

Table 11-138: Dispute Condition 13.8: Original Credit Transaction Not Accepted – Dispute Response Processing Requirements

Dispute Condition 13.8: Original Credit Transaction Not Accepted Supporting Documentation/Certification	Country/Region
Evidence that either: • A Reversal issued by the Merchant was not addressed by the Issuer in the Dispute • The Dispute is invalid	All

---

ID# 0030359	Edition: Apr 2020	Last Updated: Apr 2018

11.10.10   Dispute Condition 13.9: Non-Receipt of Cash

11.10.10.1 Dispute Condition 13.9: Non-Receipt of Cash – Dispute Reasons

An Issuer may initiate a Dispute under Dispute Condition 13.9: Non-Receipt of Cash for the following reason:

Table 11-139: Dispute Condition 13.9: Non-Receipt of Cash – Dispute Reasons

Dispute Condition 13.9: Non-Receipt of Cash Dispute Reasons	Country/Region
The Cardholder participated in the Transaction and did not receive cash or received a partial amount.	**All**

ID# 0030360	Edition: Apr 2020	Last Updated: Apr 2020

11.10.10.2 Dispute Condition 13.9: Non-Receipt of Cash – Dispute Rights

Table 11-140: Dispute Condition 13.9: Non-Receipt of Cash – Dispute Rights

Dispute Condition 13.9: Non-Receipt of Cash Dispute Rights	Country/Region
The Dispute is limited to the amount not received	**All**

ID# 0030361	Edition: Apr 2020	Last Updated: Apr 2020

11.10.10.3 Dispute Condition 13.9: Non-Receipt of Cash – Invalid Disputes

A Dispute is invalid under Dispute Condition 13.9: Non-Receipt of Cash for the following:

Table 11-141: Dispute Condition 13.9: Non-Receipt of Cash – Invalid Disputes

Dispute Condition 13.9: Non-Receipt of Cash Invalid Disputes	Country/Region
• A Cash-In Transaction • A Cash-Out Transaction	**All**

Table 11-141: Dispute Condition 13.9: Non-Receipt of Cash – Invalid Disputes (continued)

Dispute Condition 13.9: Non-Receipt of Cash Invalid Disputes	Country/Region
• A Transaction that the Cardholder states is fraudulent • A Transaction that was processed more than once	

ID# 0030362	Edition: Apr 2020 | Last Updated: Apr 2020

11.10.10.4 Dispute Condition 13.9: Non-Receipt of Cash – Dispute Time Limit

An Issuer may initiate a Dispute under Dispute Condition 13.9: Non-Receipt of Cash according to the following time limits, if applicable:

Table 11-142: Dispute Condition 13.9: Non-Receipt of Cash – Dispute Time Limit

Dispute Condition 13.9: Non-Receipt of Cash Dispute Time Limit	Country/Region
120 calendar days from the Transaction Processing Date	**All**
120 calendar days from either: • The Transaction Processing Date • For an Adjustment of an ATM Cash Disbursement or a PIN-Authenticated Visa Debit Transaction, the Transaction Date of the Adjustment	**US Domestic**

ID# 0030363	Edition: Apr 2020 | Last Updated: Apr 2020

11.10.10.5 Dispute Condition 13.9: Non-Receipt of Cash – Dispute Processing Requirements

An Issuer must provide the following documentation or certification for a Dispute under Dispute Condition 13.9: Non-Receipt of Cash:

Table 11-143: Dispute Condition 13.9: Non-Receipt of Cash – Dispute Processing Requirements

Dispute Condition 13.9: Non-Receipt of Cash Supporting Documentation/Certification	Country/Region
Certification that either:	**All**

Table 11-143: Dispute Condition 13.9: Non-Receipt of Cash – Dispute Processing Requirements (continued)

Dispute Condition 13.9: Non-Receipt of Cash Supporting Documentation/Certification	Country/Region
• The Cardholder did not receive cash • The Cardholder received partial cash and the amount the Cardholder received A Cardholder letter, if both: • The Cardholder has disputed 3 or more Transactions for non-receipt of cash at the same ATM or load device. • The disputed Transactions all occurred within the same 30-calendar day period.	

ID# 0030364	Edition: Apr 2020 | Last Updated: Apr 2020

11.10.10.6 Dispute Condition 13.9: Non-Receipt of Cash – Dispute Response Processing Requirements

An Acquirer must provide the following documentation or certification for a Dispute Response under Dispute Condition 13.9: Non-Receipt of Cash:

Table 11-144: Dispute Condition 13.9: Non-Receipt of Cash – Dispute Response Processing Requirements

Dispute Condition 13.9: Non-Receipt of Cash Supporting Documentation/Certification	Country/Region

Evidence of one of the following:
 	
 • A credit or Reversal issued by the Merchant was not addressed by the Issuer in the Dispute.
 	
 • The Dispute is invalid.
 	
 • The Cardholder no longer disputes the Transaction.
 	
 • A copy of the ATM Cash Disbursement Transaction containing at least the following:
 	
   – Payment Credential
 	
   – Transaction time or sequential number that identifies the individual Transactions
	All

Table 11-144: Dispute Condition 13.9: Non-Receipt of Cash – Dispute Response Processing Requirements (continued)

Dispute Condition 13.9: Non-Receipt of Cash Supporting Documentation/Certification	Country/Region
– Indicator that confirms that the ATM Cash Disbursement was successful	

ID# 0030365   **Edition: Apr 2020 | Last Updated: Apr 2020**

11.11   Arbitration

11.11.1   Required Documentation for Arbitration

When seeking Arbitration, a Member must provide, in English, the information required in the Visa Resolve Online Questionnaire for each Transaction, and all relevant supporting documentation.

A Member must not submit documentation or information to Visa that was not previously submitted to the opposing Member.

If the Member was not required to use VisaNet or Visa Resolve Online (VROL) to process the financial message, as specified in *Section 11.3.1, Use of Visa Systems for Dispute Processing*, the Member must provide the following, in an electronic form, with the Arbitration:

- Evidence that the dispute requirements were met for each stage of the dispute cycle
- The following internal records:[1]
    - Authorization, if authorization was attempted
    - Fraud Report (for Dispute Category 10)
    - Transaction record
    - Financial records for each stage of the dispute where a financial message was sent

[1] All records must include a key to explain the data fields. This explanation must be provided in English, or accompanied by an English translation

ID# 0030225   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.12   Compliance

11.12.1   Compliance Filing Conditions

Unless otherwise specified, a Member may file for Compliance if all of the following occur:

- A violation of the Visa Rules occurred that is not related to an Account Data Compromise Event.

- The Member has no Dispute, Dispute Response, or pre-Arbitration right.

- The Member incurred or will incur a financial loss as a direct result of the violation.[1]

- The Member would not have incurred the financial loss had the violation not occurred.[1]

- The Member made a pre-Compliance attempt to resolve the dispute with the opposing Member and the opposing Member does not accept financial liability.

The pre-Compliance attempt must include all of the following:

- Planned Compliance filing date

- All pertinent documentation

- Specific violation of the Visa Rules

[1] This does not apply to a US Credit Card Surcharge violation, as specified in *Section 11.12.4, Compliance Right for Improperly Assessed Surcharge – US Region and US Territories*

ID# 0030226   **Edition: Apr 2020 | Last Updated: Apr 2018**

11.12.2   Compliance Time Limits

A Member must not exceed the time limits specified for Compliance, as follows:

Table 11-145: Pre-Compliance Time Limits

Process Step	Time Limit
Make pre-Compliance Attempt	Either: • At least 30 calendar days before filing for Compliance • For a Dispute in which Visa Resolve Online (VROL) prevented a change of Dispute category, 29 calendar days from the Processing Date of the pre-Arbitration attempt
Accept financial responsibility and credit requesting Member	30 calendar days from the pre-Compliance attempt date

Table 11-146: Compliance Time Limits

Process Step	Time Limit
File for a Transaction not involving a fraudulent credit	90 calendar days[1] from one of the following:

Table 11-146: Compliance Time Limits (continued)

Process Step	Time Limit
	• Processing Date • Violation Date • Date the Member discovered that a violation occurred (not to exceed 2 years from the Transaction Date), if no evidence of the violation was previously available to the Member[2]
File for a Transaction involving a fraudulent credit	90 calendar days[1] from the later of either: • Processing Date of the credit Reversal • Processing Date of the use of the funds that relate to the fraudulent Credit Transactions
File for a Dispute in which VROL prevented a change of Dispute category	60 calendar days from the Processing Date of the pre-Arbitration attempt
[1] Plus 30 calendar days for a Group Member [2] A Member must provide evidence that this was the date on which the financial loss was discovered.	

11.12.3   Compliance Conditions and Required Documentation

When seeking Compliance, a Member must provide all of the following:

- The information required in the Visa Resolve Online Questionnaire for each Transaction

- Documentation substantiating that a financial loss would not have resulted if the violation had not occurred. Documentation must be provided in English or accompanied by an English translation.

- If applicable, the documentation shown in the tables in this section

- Other relevant supporting documentation

A Member must not submit documentation or information to Visa that was not previously submitted to the opposing Member.

Table 11-147: Chargeback Reduction Service Returned or VROL Prevented Valid Dispute, Dispute Response, or Pre-Arbitration Attempt for Invalid Data

Compliance Condition
The Chargeback Reduction Service returned or Visa Resolve Online (VROL) prevented a valid Dispute,[1] Dispute Response, or pre-Arbitration attempt resulting from a Member transmitting invalid data.
Required Documentation
Both: • Evidence of incorrect or invalid data • Evidence that the Member was able to meet the conditions for a Dispute, Dispute Response, or pre-Arbitration attempt
Compliance Condition
The Chargeback Reduction Service returned a Transaction with a valid Authorization.
Required Documentation
All of the following: • The Transaction Receipt • Evidence that the Transaction received an Authorization • Evidence of the Chargeback Reduction Service return
[1] This includes Transactions for which the Issuer has previously initiated a Dispute under Dispute category 10 (Fraud) or 11 (Authorization) based on invalid data but is prevented by VROL from continuing the dispute using Dispute category 12 (Processing Errors) or 13 (Consumer Disputes).

Table 11-148: Unauthorized Signature

Compliance Condition
A Cardholder's account was charged for a Transaction and all of the following: • The Cardholder denies authorizing or participating in the Transaction. • The Card that was lost or stolen, and recovered, was used in the disputed Transaction. • The first initial of the first name or the last name of the signature on the Transaction Receipt is not the same as the signature on the Card signature panel. • The Transaction was not one of the following:

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-148: Unauthorized Signature (continued)

Compliance Condition
– Vehicle-Specific Fleet Card Transaction   – Emergency Cash Disbursement   – Priority check-out Transaction at a Lodging Merchant   – Transaction using a Contactless Device that is not a standard plastic Card   – An emergency travelers Cheque refund   This does not apply to a Transaction that takes place either at a Compliant Chip Card Reading Device or on a Card that does not have a signature panel.
Required Documentation

• Certification, completed Visa Resolve Online Questionnaire, stating both:
 	
    – That the Cardholder denies authorizing or participating in the Transaction
 	
    – That the recovered Card signature panel was unaltered and describing the Card recovery circumstances
 	
 • Transaction Receipt
 	
 • Copy of the front and back of the recovered Card

Table 11-149: Cardholder Letter Required for Legal Purposes

Compliance Condition
An Acquirer or Merchant requires a signed Cardholder letter for legal proceedings, for a law enforcement investigation, or if required by applicable laws or regulations.
Required Documentation
Either: • Evidence that the signed Cardholder letter is required for legal proceedings (for example: court order or subpoena)   • Evidence that the Cardholder letter is required for a law enforcement investigation

---

Table 11-150: Copy of Transaction Receipt

Compliance Condition
An Issuer or a Cardholder requires a copy of the Transaction Receipt for legal proceedings or a law enforcement investigation and a valid Retrieval Request for a copy bearing signature was made within 120 calendar days of the Transaction Processing Date. An Issuer may file a pre-Compliance case if it has made a valid Retrieval Request for a copy bearing signature within 120 calendar day of the Transaction Processing Date and the Acquirer has not provided a valid response to the Retrieval Request. An Issuer must not file the pre-Compliance case if it has either: • Reported Fraud Activity for the Transaction. • Listed the Account Number on the Exception File on or after the Transaction Date.
Required Documentation
One of the following: • Evidence that the Transaction Receipt is required for legal proceedings (for example: court order or subpoena) • For the purpose of legal proceedings, evidence that the Transaction Receipt is required for legal proceedings (for example: court order or subpoena) or for a law enforcement investigation • For the purpose of an investigation by the Issuer, certification from the Issuer both that a signed Transaction Receipt is needed in order to respond to Cardholder escalation, and the reason for the escalation

Table 11-151: Authorization Received after Decline Response on Counterfeit Card

Compliance Condition
All of the following: • An Authorization Request for a Magnetic Stripe-read or Chip-initiated Transaction received a Decline Response or a Pickup Response • A subsequent Authorization was obtained by a means other than Voice Authorization. • The Merchant completed the Transaction. • The Transaction was initiated with a Counterfeit Card.
Required Documentation

Visa Product and Service Rules

11 Dispute Resolution

Visa Core Rules and Visa Product and Service Rules

Table 11-151: Authorization Received after Decline Response on Counterfeit Card (continued)

Compliance Condition
Certification that the approved Transaction was counterfeit and both the initial and subsequent Authorization Requests contained all of the following identical data: • Payment Credential • Transaction Date • Transaction amount • Merchant identification

Table 11-152: Fraudulent Multiple Transactions

Compliance Condition
All of the following: • The Cardholder denies authorizing or participating in one or more Card-Present Environment Transactions. • The Cardholder acknowledges participating in at least one Transaction. • All of the Transactions were key-entered in a Card-Present Environment and occurred at the same Merchant Outlet and on the same date. • The Card was in the Cardholder's possession at the time of the disputed Transactions. • The Issuer has not reported Fraud Activity on the Payment Credential using fraud type code 3 (fraudulent application)
Required Documentation
Both: • A Cardholder letter • If the acknowledged Transaction was not processed, the Cardholder copy of the Transaction Receipt

Table 11-153: Counterfeit Card Transaction with Incomplete Data

Compliance Condition
All of the following: • The Transaction was completed with a Counterfeit Card in a Card-Present Environment.

Table 11-153: Counterfeit Card Transaction with Incomplete Data (continued)

Compliance Condition
• The Cardholder denies authorizing or participating in the Transaction. • CVV was encoded on the Card. • The Transaction was not completed with a Proprietary Card bearing the Plus Symbol. • Online Authorization was obtained without transmission of the entire unaltered data on track 1 or track 2 of the Magnetic Stripe. • The Issuer reported Fraud Activity to Visa for the Transaction using fraud type code 4. • **Effective for pre-Compliance attempts processed on or after 20 April 2020** The Transaction was not an ATM Cash Disbursement.
Required Documentation

• All of the following, as applicable:
 	
  – Certification that the CVV was encoded on the Card
 	
  – Certification that the Issuer was a participant in the Card Verification Service at the time of Authorization
 	
  – Cardholder letter denying authorization of or participation in the Transaction

Table 11-154: Fraudulent Credits

Compliance Condition
All of the following: • The Issuer has attempted but is unable to obtain funds from the Cardholder • The account is no longer in use • A Credit Transaction was applied to the account without any prior Transactions • The available credits were withdrawn from the account • Credit reversals were processed. This does not apply to the following: • An Original Credit Transaction • Accounts that are still in use

Table 11-154: Fraudulent Credits (continued)

Compliance Condition
Required Documentation
All of following: • The date(s) of the Credit Transaction(s) • The date(s) of the Credit Reversal(s) • The date(s) of fraudulent sale(s) or withdrawal(s). If the withdrawal was not made with the Card, the Issuer must supply evidence of the withdrawal. • Evidence that the withdrawal of funds from a Cardholder's account results in a negative or zero balance • An explanation on why the Issuer is unable to collect from the Cardholder

Table 11-155: Shared Deposit – No Documentation Received for Deposit Return Item

Compliance Condition
The Acquirer processed an Adjustment for a returned Shared Deposit, but the returned deposit item documentation was not received by the Issuer within 10 calendar days of the Adjustment.
Required Documentation
Issuer certification that the returned deposit item documentation was not received within 10 calendar days

Table 11-156: Shared Deposit – Cardholder Did Not Receive Credit or Settlement Amount Did Not Match

Compliance Condition
The Cardholder made a deposit and either: • The Cardholder did not receive credit for the deposit • The Settlement amount did not match the deposit amount
Required Documentation
Issuer certification of either: • The Cardholder did not receive credit for the deposit • The amount deposited and the correct deposit amount

Table 11-157: ATM Adjustment for Fraudulent Transactions

Compliance Condition
Effective for Transactions completed on or after 18 April 2020 All of the following:
• Fraudulent ATM Transactions were processed on the same Transaction Date to the same Payment Credential by the same Acquirer, and subsequently reversed.
• The reason code for the Reversal was either:
– 2502 (Transaction has not completed [request or advice timed out or ATM malfunctioned])
– 2503 (No confirmation from point of service)
• The Acquirer processed debit Adjustments for more than 2 of the reversed ATM Transactions.
• The Issuer has reported the Fraud Activity to Visa.
• The Issuer has attempted but is unable to obtain funds from the Cardholder.
• The Payment Credential is no longer in use
Required Documentation
Effective for Transactions completed on or after 18 April 2020 Both:
• Issuer certification of all of the following:
– Date and amounts of the ATM Transactions
– Date and amounts of the ATM Transaction Reversals
– Date and amounts of the ATM debit Adjustments
– An explanation of why the Issuer is unable to collect funds from the Cardholder
• Evidence that the debit Adjustment resulted in a negative or zero balance on the account

ID# 0030228   Edition: Apr 2020 | Last Updated: Apr 2020

11.12.4   Compliance Right for Improperly Assessed Surcharge – US Region and US Territories

A Member may file for Compliance if a Merchant in the US Region or in a US Territory assessed a US Credit Card Surcharge under one of the following conditions:

• US Credit Card Surcharge amount exceeds the applicable US Credit Card Surcharge amount as specified in the Visa Rules

- US Credit Card Surcharge was assessed on a Transaction in a manner that does not comply with the Visa Rules

- US Credit Card Surcharge was assessed on a Transaction type where surcharging is not permitted

- US Credit Card Surcharge was assessed by a third party

- US Credit Card Surcharge was not disclosed as specified in the Visa Rules

- US Credit Card Surcharge amount did not appear on the Transaction Receipt as specified in the Visa Rules

- US Credit Card Surcharge amount was not refunded as specified in the Visa Rules

- For a Dynamic Currency Conversion Transaction, US Credit Card Surcharge amount was not included in the conversion

- Convenience Fee, Service Fee, currency conversion fee, commission, or Wire Transfer Money Order service fee was applied on a Transaction that included a US Credit Card Surcharge

The Member must only request Compliance for the US Credit Card Surcharge amount.

The Member is not required to have incurred a financial loss as a direct result of the violation. If the Issuer has billed the Transaction that included the US Credit Card Surcharge to the Cardholder, the Issuer must credit the Cardholder for the US Credit Card Surcharge amount.

A Member must not file for Compliance if the Merchant properly assessed a US Credit Card Surcharge as permitted in the Visa Rules.

ID# 0030229	Edition: Apr 2020 | Last Updated: Apr 2018

11.12.5   Data Compromise Recovery

A violation involving failure to comply with the PIN Management Requirements Documents, *Visa PIN Security Program Guide*, or Payment Card Industry Data Security Standard (PCI DSS) that could allow a compromise of Magnetic-Stripe Data is not resolved through the Compliance process. Such violations are resolved through the Global Compromised Account Recovery program.

ID# 0030230	Edition: Apr 2020 | Last Updated: Apr 2018

11.13   Arbitration and Compliance Decision

11.13.1   Arbitration and Compliance Filing Authority

An Arbitration or Compliance request must be filed with either:

- The requesting Member's Group Member

- Visa

If the Group Member determines that a request is invalid, it must return the request to the requesting Member. The requesting Member must not seek recourse with Visa.

ID# 0030366	Edition: Apr 2020	Last Updated: Apr 2018

11.13.2   Use of V.I.P. System Authorization Records in Arbitration and Compliance

If the Issuer's and Acquirer's Authorization records for a Transaction do not match, the V.I.P. System Authorization record prevails at Arbitration and Compliance.[1]

[1] In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region* it must refer to *Visa Europe Operating Regulations – Processing*.

ID# 0030368	Edition: Apr 2020	Last Updated: Apr 2018

11.13.3   Withdrawal of an Arbitration or Compliance Case

The Member may withdraw its Arbitration or Compliance request within 7 calendar days from the Visa acknowledgement date and will be assigned financial liability.

If a case is withdrawn, Visa will debit or credit through Visa Resolve Online (VROL) the Member accepting responsibility, if necessary, based on the final determination of responsibility for the Dispute amount.

ID# 0030370	Edition: Apr 2020	Last Updated: Apr 2018

11.13.4   Conditions for an Appeal to the Arbitration and Compliance Committee

A Member may appeal a decision by the Arbitration and Compliance Committee only if both:

- The Member can provide new evidence not previously available at the time the original case was filed.

- The disputed amount is at least USD 5,000 (or local currency equivalent).

ID# 0030373	Edition: Apr 2020	Last Updated: Apr 2018

11.13.5   Appeal Time Limit

The adversely affected Member must file any appeal within 60 calendar days of the Notification date of the decision by the Arbitration and Compliance Committee.

ID# 0030374	Edition: Apr 2020 | Last Updated: Apr 2018

11.13.6   Appeal Review Fee

The requesting Member must not collect the review fee from the opposing Member if the original decision is reversed.

ID# 0030375	Edition: Apr 2020 | Last Updated: Apr 2020

11.14   Retrieval Request and Fulfillment

11.14.1   Retrieval Request Information Requirements

A Retrieval Request must contain all of the following information:

- Acquirer Reference Number
- Payment Credential
- Transaction Date of original Presentment
- Merchant Category Code (MCC)
- Either the Transaction Amount in the Transaction Currency or a complete description of the Merchant's business
- Applicable Retrieval Request reason code

ID# 0030231	Edition: Apr 2020 | Last Updated: Apr 2020

11.14.2   Retrieval Request Fulfillment Requirements

An Issuer may submit a Retrieval Request for a Transaction only if all of the following apply:

- The Transaction occurs in a Face-to-Face Environment.
- The Transaction takes place at a Magnetic-Stripe-only Acceptance Device.
- The Transaction is not a Visa Easy Payment Service (VEPS) Transaction.
- A PIN was not obtained.
- The Card has a signature panel.

An Acquirer must fulfill a Retrieval Request if both of the following apply:

- The Retrieval Request is received within 120 calendar days from the Processing Date.
- The Transaction is not invalid, as specified in *Table 11-158, Retrieval Request – Allowable Nonfulfillment Transaction Types*.

To fulfill a Retrieval Request, an Acquirer must provide documentation within 30 days of receipt of the Retrieval Request, as follows:

- The Merchant or Acquirer copy of the Transaction Receipt bearing the signature that was used to verify the Cardholder. An Acquirer may reproduce the Cardholder signature obtained using an electronic capture device.
- In the US Region: For Preauthorized Health Care Transaction, a copy of the Order Form

A Fulfillment must comply with all of the following:

- Be legible enough for the Cardholder to read or for the Issuer to identify the Payment Credential
- Include either:
  - The unique 12-digit identifier assigned by VisaNet[1] to a request for a Transaction Receipt copy
  - In the Europe Region: The Copy Request Identifier
- For a US Domestic Transaction, include a unique 9-digit control number assigned by the Issuer to identify the source of the request[1]

An Acquirer may send a Nonfulfillment Message for a Transaction as follows:

Table 11-158: Retrieval Request – Allowable Nonfulfillment Transaction Types

Region	Invalid Transaction Type
All	A Transaction for which the Issuer received a signed Transaction Receipt through the Visa Merchant Purchase Inquiry system

All	Any of the following:
	
	- A Transaction that takes place at a Compliant Chip Card Reading Device.
	- A Transaction that takes place in a Face-to-Face Environment at a Magnetic-Stripe-only Acceptance Device and either:
	  - A PIN was obtained.
	  - The Transaction was a Visa Easy Payment Service (VEPS) Transaction.
	- A Transaction that takes place using a Card that does not contain a signature panel.

LAC Region (Brazil)	Domestic Transactions

¹ In the US Region: This does not apply to a copy request for a Healthcare Auto-Substantiation Transaction.

ID# 0030232	Edition: Apr 2020 | Last Updated: Apr 2020

11.14.3   Retrieval Request Prohibition

An Issuer must not submit a Retrieval Request for a Transaction for any of the following:

- Takes place at a Compliant Chip Card Reading Device
- Takes place at a Magnetic-Stripe-only Acceptance Device and either:
  - A PIN was obtained.
  - The Transaction was a Visa Easy Payment Service (VEPS) Transaction.
- Where the Card does not have a signature panel

ID# 0030552	Edition: Apr 2020 | Last Updated: Oct 2019

12   Fees and Non-Compliance Assessments

12.2   Issuance Non-Compliance Assessments

12.2.1   Fraud Activity Reporting Non-Compliance Assessments

12.2.1.1   Issuer Fraud Activity Reporting Non-Compliance Assessments

If an Issuer does not comply with the fraud reporting requirements specified in *Section 1.10.4.3, Issuer Fraud Activity Reporting,* the Issuer is subject to non-compliance assessments, as follows:

Table 12-1: Non-Compliance Assessments for Failure to Report Fraud

Occurrence[1]	Warning Letter	Suspension of Fraud Dispute Rights[2]	Non-Compliance Assessment (Minimum Amount)	Onsite Member Audit
First	Yes	N/A	USD 0	N/A
Second	Yes	N/A	USD 0	N/A
Third	N/A	90 calendar days	USD 25,000	N/A
Fourth	N/A	180 calendar days	USD 25,000, or, in the Europe Region, USD 50,000	Yes
Fifth	N/A	Indefinite until compliance achieved	Visa decision based on reevaluation	N/A
[1] In the Europe Region: After the first occurrence applies to consecutive calendar quarters				
[2] Dispute conditions will be determined by Visa.				

In the Europe Region: In addition, Visa may monitor the Issuer for 8 quarters.

ID# 0028308   Edition: Apr 2020 | Last Updated: Apr 2018

12.2.1.2   Chip Interoperability Compliance Program Non-Compliance Assessments

A Member is subject to the non-compliance assessments specified in *Table 12-2, Member Non-Compliance Assessments for Non-Compliance with the Chip Interoperability Compliance Program –*

Visa Product and Service Rules

12 Fees and Non-Compliance Assessments

Visa Core Rules and Visa Product and Service Rules

AP Region, Canada Region, CEMEA Region, LAC Region, US Region, or, in the Europe Region, *Table 12-3, Member Non-Compliance Assessments for Non-Compliance with the Chip Interoperability Compliance Program – Europe Region,* if Visa determines that the Member or its agent has violated the Chip Interoperability Compliance Program by failing to do one of the following:

- Establish and commit to an agreed Chip interoperability resolution plan

- Make satisfactory progress toward resolution under an agreed Chip interoperability resolution plan[1]

- In the Europe Region: Fail to undertake or successfully complete testing with the Acquirer Device Validation Toolkit (ADVT)

Table 12-2: Member Non-Compliance Assessments for Non-Compliance with the Chip Interoperability Compliance Program – AP Region, Canada Region, CEMEA Region, LAC Region, US Region

Violation	Month	Visa Action, Notification, or Non-Compliance Assessment
Initial identification and confirmation of a violation	Month 1	Member receives Notification that Visa will take action if the situation is not addressed to the satisfaction of Visa within 30 calendar days
Unaddressed violation	Month 2	Visa discontinues any Member incentives associated with deployment of products that have been identified as contributors to interoperability problems. Visa may also suspend other incentives. Visa issues a second Notification that non-compliance assessments may apply if the situation is not corrected to the satisfaction of Visa within 60 calendar days of the second Notification.
Unaddressed violation	Months 4-5	Member is assessed USD 25,000 per month
Unaddressed violation	Month 6 and subsequent months	Member is assessed USD 50,000 per month

Table 12-3: Member Non-Compliance Assessments for Non-Compliance with the Chip Interoperability Compliance Program – Europe Region

Violation	Action or Non-Compliance Assessment
Initial identification and confirmation of a	The Member must commit to a resolution plan agreed with Visa

Visa Product and Service Rules

12 Fees and Non-Compliance Assessments

Visa Core Rules and Visa Product and Service Rules

Table 12-3: Member Non-Compliance Assessments for Non-Compliance with the Chip Interoperability Compliance Program – Europe Region (continued)

Violation	Action or Non-Compliance Assessment
Chip interoperability problem.	to resolve the Chip interoperability problem within 30 calendar days of notification that it may be assessed a non-compliance assessment.
Either: • Agreed resolution plan not provided to Visa • Agreed resolution plan not followed within 30 calendar days of initial notification	EUR 10,000 non-compliance assessment
Either: • Agreed resolution plan not provided to Visa • Agreed resolution plan not followed within 60 calendar days of initial notification	EUR 50,000 non-compliance assessment
Either: • Agreed resolution plan not provided to Visa • Agreed resolution plan not followed within 90 calendar days of initial notification	EUR 100,000 non-compliance assessment
Either: • Agreed resolution plan not provided to Visa • Agreed resolution plan not followed within 120 calendar days of initial notification	EUR 100,000 non-compliance assessment and EUR 100,000 per subsequent month and the case will be reviewed for further action at Visa's discretion

[1] In the Europe Region: Including provision of progress reports to Visa

ID# 0001292   Edition: Apr 2020 | Last Updated: Oct 2016

12.3   Acceptance Non-Compliance Assessments

12.3.1   EMV Liability Shift and Fallback Non-Compliance Assessments

12.3.1.1   Global Fallback Monitoring Program Identification Non-Compliance Assessments

An Acquirer is subject to a non-compliance assessment of USD 1 per Fallback Transaction when the Acquirer-country combination meets or exceeds the minimum Transaction volume and percentage parameters specified in the Visa Rules and the *Global Chip Fallback Monitoring Program Guide*.[1]

Transactions involving Acquirers in the Europe Region will be subject to a non-compliance assessment of EUR 1 per Fallback Transaction.

[1] In the AP Region (Japan): This does not apply to Account Number Verification Transactions processed as Magnetic-Stripe Transactions.

ID# 0008405	Edition: Apr 2020 | Last Updated: Oct 2016

12.3.2   High-Risk Internet Payment Facilitator Non-Compliance Assessments

12.3.2.1   High-Risk Internet Payment Facilitator Registration Non-Compliance Assessments

An Acquirer that fails to comply with the registration program requirements for High-Risk Internet Payment Facilitators is subject to a non-compliance assessment,[1] as follows:

- USD 25,000 per month per High-Brand Risk Sponsored Merchant or High-Risk Internet Payment Facilitator

- After 3 violations in a calendar year, one or both of the following:
    - USD 100,000 for each 30-calendar-day period of non-compliance
    - Prohibition against signing High-Brand-Risk Sponsored Merchants

[1] **Effective 18 April 2020** In the Europe Region

ID# 0026334	Edition: Apr 2020 | Last Updated: Apr 2020

12.3.3   Chip Card Non-Compliance Assessments

12.3.3.1   Visa Debit Acquirers Compliance Program Non-Compliance Assessments – Canada Region

Effective through 17 April 2020 In the Canada Region: An Acquirer that fails to update its host systems with the ability to process Visa Debit Category Transactions will be subject to a non-compliance assessment of CAD 100,000 per month of non-compliance. If an Acquirer or its Visa Debit Acceptor fails to properly process Visa Debit Category Transactions, the Acquirer will be subject to a non-compliance assessment of CAD 5,000 per Cardholder complaint reported to Visa as an Acceptance Compliance Program incident.

Effective 18 April 2020 In the Canada Region: An Acquirer that fails to update its host systems with the ability to process Visa Debit Category Transactions will be subject to the non-compliance assessments specified in the Tier 1 schedule in *Section 1.12.2.2, General Non-Compliance Assessment Schedules.* If an Acquirer or its Visa Debit Acceptor fails to properly process Visa Debit Category Transactions, the Acquirer will be subject to a non-compliance assessment specified in the Tier 2 schedule in *Section 1.12.2.2, General Non-Compliance Assessment Schedules* per Cardholder complaint reported to Visa as an Acceptance Compliance Program incident.

ID# 0008364	Edition: Apr 2020	Last Updated: Apr 2020

12.3.4   Marketplace Non-Compliance Assessments

12.3.4.1   Marketplace Non-Compliance Assessments

Effective 18 April 2020 Visa will impose non-compliance assessments on an Acquirer that fails to meet Marketplace requirements, as follows:

Table 12-4: Non-Compliance Assessments for Member Failure to Meet Marketplace Requirements

Violation	Visa Action/Non-Compliance Assessment
Initial failure to meet Marketplace requirements	Warning letter issued and non-compliance assessment of USD 25,000
30 calendar days have passed after response due and the initial failure has not been corrected	USD 50,000
60 calendar days have passed after response due and the initial failure has not been corrected	USD 100,000

Table 12-4: Non-Compliance Assessments for Member Failure to Meet Marketplace Requirements (continued)

Violation	Visa Action/Non-Compliance Assessment
90 calendar days have passed after response due and the initial failure has not been corrected	USD 150,000
120 calendar days have passed after response due and the initial failure has not been corrected	USD 200,000
150 calendar days have passed after response due and the initial failure has not been corrected	USD 250,000 Non-compliance assessments will continue to be levied each month until the rule violation is corrected, with the amount increasing at Visa discretion.

ID# 0030659   Edition: Apr 2020 | Last Updated: Oct 2019

12.3.5   Mass Transit Non-Compliance Assessments

12.3.5.1   Mass Transit Transaction Processing Non-Compliance Assessments – Europe Region

In the Europe Region: An Acquirer may be subject to a non-compliance assessment of EUR 30 for each Mass Transit Transaction processed incorrectly by its Merchants.

ID# 0030055   Edition: Apr 2020 | Last Updated: Apr 2018

12.3.6   Dynamic Currency Conversion (DCC)

12.3.6.1   Dynamic Currency Conversion Non-Compliance Assessments

Visa may, at its discretion, audit Acquirers and their Merchants to ensure compliance with the Dynamic Currency Conversion (DCC) requirements. If the result of an audit identifies any Merchant Outlet or ATM violation, the Acquirer is subject to both:

- A non-refundable non-compliance assessment of up to USD 10,000

- A non-compliance assessment of up to USD 25,000 per month, where payment will be deferred until a follow-up audit confirms that all violations have been corrected. If the violations continue, all deferred non-compliance assessments will be immediately levied.

ID# 0030703	Edition: Apr 2020 | Last Updated: New

12.5   Transaction Processing Non-Compliance Assessments

12.5.1   Authorization and Clearing Non-Compliance Assessments

12.5.1.1   Online Gambling Transaction Identification Non-Compliance Assessment

Effective through 17 April 2020 An Acquirer is subject to the non-compliance assessments specified in *Section 12.6.9, Global Brand Protection Program Non-Compliance Assessments,* if an Authorization Request for an Online Gambling Transaction contains incorrect data or fails to include all of the following:

- An appropriate MCC to identify the High-Brand Risk Merchant, as specified in *Section 10.4.6.1, High-Brand Risk Merchants*

- MCC 7995 (Betting), for an Online Gambling Transaction, as specified in *Section 5.9.17.1, Online Gambling Merchant and Acquirer Requirements*

- POS Condition Code 59

Effective through 17 April 2020 In the Europe Region: Visa may prohibit an Acquirer from contracting with a new Online Gambling Merchant for a period of one year or more if one or more of that Acquirer's Online Gambling Merchants are identified as failing to comply with this requirement for a period of 4 or more months during any 12–month period.

ID# 0008753	Edition: Apr 2020 | Last Updated: Apr 2020

12.6   Risk Non-Compliance Assessments

12.6.1   Account and Transaction Information Security Non-Compliance Assessments

12.6.1.1   Account Information Security Program Non-Compliance Assessments

A Member deemed non-compliant with the Account Information Security Program is subject to a non-compliance assessment, as follows:

Table 12-5: Non-Compliance Assessments for the Account Information Security Program – AP Region, Canada Region, CEMEA Region, LAC Region, US Region

Violation	Non-Compliance Assessment
First violation	Up to USD 50,000
Second violation	Up to USD 100,000
Third or any subsequent violation	Up to USD 200,000

Table 12-6: Non-Compliance Assessments for the Account Information Security Program – Europe Region

Violation	Visa Action or Non-Compliance Assessment
First violation of rule	Warning letter with specific date for correction and USD 500 non-compliance assessment
Second violation of same rule in a 12-month period after date of correction specified in Notification of first violation	USD 5,000 non-compliance assessment
Third violation of same rule in a 12-month period after date of correction specified in Notification of first violation	USD 10,000 non-compliance assessment
Fourth violation of same rule in a 12-month period after date of correction specified in Notification of first violation	USD 25,000 non-compliance assessment
Five or more violations of same rule in a 12-month period after date of correction specified in Notification of first violation	At Visa discretion
If the 12-month period is not violation-free and the non-compliance assessments total USD 25,000 or more	Additional non-compliance assessments equal to all non-compliance assessments levied during that 12-month period

ID# 0008193   **Edition: Apr 2020 | Last Updated: Apr 2019**

12.6.1.2   Non-Compliance Assessments for Account and Transaction Information Security Requirements

If Visa determines that a Member, its agent, or a Merchant has been deficient or negligent in securely maintaining account or Transaction Information, or reporting or investigating the loss of this information, Visa may impose a non-compliance assessment on the Member or require the Member to take immediate corrective action.

In the Europe Region: An Acquirer that does not have 90% of its Merchants in each of the following categories in compliance with account information and Transaction Information security requirements must provide Visa, for each non-compliant Merchant type, an explanation and a plan for the next 12 months, indicating how it will ensure the protection of Cardholder data:

- Level 1 (more than 6 million Transactions per year)
- Level 2 (1,000,001 – 6 million Transactions per year)
- Level 3 (Electronic Commerce Merchants with 20,000 – 1 million Transactions per year)
- Level 4 (1 – 1 million Transactions per year)

The Acquirer must do all of the following:

- Report to Visa its compliance with the Payment Card Industry Data Security Standard (PCI DSS)
- Report and verify to Visa, at least every 6 months, its Merchants' status of PCI DSS compliance
- Ensure that its level 3 and 4 Electronic Commerce Merchants either:
  - Exclusively use a service provider that is PCI DSS-compliant
  - Provide to the Acquirer certification of the Merchant's PCI DSS compliance
- Ensure that its level 1 and 2 Merchants and its Airline and Lodging Merchants meet the compliance thresholds mandated by Visa

ID# 0001753   **Edition: Apr 2020 | Last Updated: Apr 2019**

12.6.1.5   Non-Compliance Assessment for Failure to Notify and Respond to Transaction Information Loss or Theft

Effective through 17 April 2020 in the AP Region, CEMEA Region, Europe Region, LAC Region, US Region, and effective through 17 July 2020 in the Canada Region: An Acquirer that fails to notify Visa immediately of the suspected or confirmed loss or theft of any Visa Transaction Information is subject to a non-compliance assessment of up to USD 100,000 per incident.

Effective 18 April 2020 in the AP Region, CEMEA Region, LAC Region, US Region, and effective 18 July 2020 in the Canada Region: A Member that fails to notify Visa immediately of the

suspected or confirmed loss or theft of any Visa Transaction Information, or fails to adequately and timely respond to the loss or theft of such information, is subject to a non-compliance assessment of up to USD 100,000 per incident, as specified in *What to Do if Compromised*.

Effective 18 April 2020 In the Europe Region: A Member is subject to a non-compliance assessment if it does not comply with requirements relating to Member cooperation to protect against data compromise, as specified in *Section 10.3.1.4, Member Cooperation to Protect Against Data Compromise – Europe Region.*

ID# 0003524   Edition: Apr 2020 | Last Updated: Apr 2020

12.6.2   Anti-Money Laundering Program Non-Compliance Assessments

12.6.2.1   Failure to Return an Anti-Money Laundering/Anti-Terrorist Financing Questionnaire Non-Compliance Assessments

Effective through 17 April 2020 In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Visa imposes non-compliance assessments for failure to return to Visa a completed *Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF), Sanctions and Anti-Bribery Compliance Program Questionnaire,* as specified in *Section 1.10.1.7, Visa Anti-Money Laundering Program – Member Requirements,* or to respond to follow-up questions or inquiries, as follows:

Table 12-7: Non-Compliance Assessments for Member Failure to Return a Completed Anti-Money Laundering/Anti-Terrorist Financing Questionnaire – AP Region, Canada Region, CEMEA Region, LAC Region, US Region

Date	Non-Compliance Assessment
Due date + one calendar day to 30 calendar days	USD 1,000
Due date + 31 calendar days to 60 calendar days	USD 2,500
Due date + 61 calendar days to 90 calendar days	USD 5,000
Due date + 91 calendar days and every 30 calendar days thereafter	USD 10,000

Effective 18 April 2020 Visa imposes non-compliance assessments specified in the Tier 2 schedule in *Section 1.12.2.2, General Non-Compliance Assessment Schedules* for failure of a Member to return to Visa a completed *Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF), Sanctions and Anti-Bribery Compliance Program Questionnaire,* as specified in *Section 1.10.1.7, Visa Anti-Money Laundering Program – Member Requirements,* or to respond to follow-up questions or inquiries.

ID# 0026362   Edition: Apr 2020 | Last Updated: Apr 2020

12.6.3   Authentication Non-Compliance Assessments

12.6.3.1   PIN Security Non-Compliance Assessments

A Member may be subject to a non-compliance assessment for its or its agent's failure to comply with any of the requirements in the PIN Management Requirements Documents and *Visa PIN Security Program Guide*, as follows:

Table 12-8: PIN Security Non-Compliance Assessments

Violation	Non-Compliance Assessment
Initial violation and each month of unaddressed violations, up to 4 months after the initial violation	USD 10,000 per month
Violations after 4 months and each month thereafter	USD 25,000 per month

If an Acquirer fails to respond to Visa within 30 days of a Notification of non-compliance, it may be subject to a non-compliance assessment, or Visa may suspend the Acquirer's certification relating to PIN implementation procedures until a response from the Acquirer has been received and acknowledged by Visa.

If the Acquirer provides an action plan to Visa but does not perform its commitments as specified in the action plan, it must deposit USD 100,000 with Visa as a performance bond or place USD 100,000 in escrow until Visa either:

- Confirms that the Acquirer is in compliance with the PIN Management Requirements Documents
- In the case of the escrow arrangements, suspends that Acquirer's certification. If Acquirer certification for PIN implementation procedures is suspended, the Acquirer may forfeit to Visa the performance bond or escrow amount.

ID# 0001288   Edition: Apr 2020 | Last Updated: Oct 2018

12.6.4   Visa Monitoring Program Non-Compliance Assessments

12.6.4.1   Visa Acquirer Monitoring Program (VAMP) Non-Compliance Assessments

Visa assesses the following non-compliance assessments if an Acquirer's monthly Dispute or Fraud Activity meets or exceeds the Visa Acquirer Monitoring Program (VAMP) thresholds specified in *Section 10.4.4.1, Visa Acquirer Monitoring Program (VAMP)*:

Table 12-9: Non-Compliance Assessments for Excessive Disputes or Fraud Activity-to-Sales Ratio

Month	Non-Compliance Assessment
Month 1 – 3	USD 25,000 (or local currency equivalent) per month
Month 4 – 6	USD 50,000 (or local currency equivalent) per month
Month 7 – 12 (and, in the Europe Region, subsequent months)	USD 100,000 (or local currency equivalent) per month

Visa may assess, suspend, or waive VAMP non-compliance assessments, in whole or in part, to accommodate unique or extenuating circumstances. The non-compliance assessments will no longer be assessed to the Acquirer once its Merchant has met acceptable performance levels. However, non-compliance assessments may continue to be assessed, or a Merchant may be prohibited from participating in the Visa Program, if Visa determines that the Merchant or Acquirer is causing undue economic hardship or harm to the goodwill of the Visa system as a result of high Dispute or Fraud Activity volumes.

In the Europe Region: If an Acquirer exceeds 3 times the monthly fraud-to-sales ratio communicated by Visa to Acquirers, Visa will determine non-compliance assessments.

ID# 0029293	Edition: Apr 2020	Last Updated: Apr 2018

12.6.4.2   Visa Issuer Monitoring Program (VIMP) Non-Compliance Assessments

Effective 19 October 2019 in the Canada Region, CEMEA Region, Europe Region, LAC Region, US Region, and effective 18 April 2020 in the AP Region Visa assesses the following non-compliance assessments if an Issuer's monthly Card-Absent Environment Fraud Activity meets or exceeds the Visa Issuer Monitoring Program (VIMP) thresholds specified in *Section 10.4.9.1, Visa Issuer Monitoring Program (VIMP)*:

Table 12-10: Non-Compliance Assessments for Excessive Fraud Activity-to-Sales Ratio

Month	Non-Compliance Assessment
Month 1 – 3	Not applicable
Month 4 – 6	USD 25,000 (or local currency equivalent) per month
Month 7 – 9	USD 50,000 (or local currency equivalent) per month
Month 10 – 12	USD 100,000 (or local currency equivalent) per month

Visa may assess, suspend, or waive VIMP non-compliance assessments, in whole or in part, to accommodate unique or extenuating circumstances. The non-compliance assessments will no longer be assessed to the Issuer once it has met acceptable performance levels. However, non-compliance assessments may continue to be assessed, or an Issuer may be prohibited from participating in the Visa Program, if Visa determines that the Issuer is causing undue economic hardship or harm to the goodwill of the Visa system as a result of high Fraud Activity volumes.

ID# 0030600	Edition: Apr 2020 | Last Updated: Apr 2019

12.6.4.3   Risk Monitoring Programs Data Quality Non-Compliance Assessments

Effective 18 April 2020 If Visa determines that an Acquirer or its Merchant changed, modified, or altered the Merchant name, Merchant data, or Merchant performance in any way to circumvent the Visa Dispute Monitoring Program (VDMP), the Visa Fraud Monitoring Program (VFMP), or the Global Brand Protection Program, Visa may impose a non-compliance assessment of USD 25,000 (or local currency equivalent) per Merchant Outlet, per month, to the Acquirer.

ID# 0030702	Edition: Apr 2020 | Last Updated: New

12.6.5   Dispute Monitoring Fees and Non-Compliance Assessments

12.6.5.1   Visa Dispute Monitoring Program (VDMP) Fees and Non-Compliance Assessments

Visa assesses Visa Dispute Monitoring Program (VDMP) fees and non-compliance assessments to the Acquirer, as specified in *Table 12-11, Fees for Visa Dispute Monitoring Program – Standard Program*, and *Table 12-12, Fees for Visa Dispute Monitoring Program – High-Risk Program*.

Table 12-11: Fees for Visa Dispute Monitoring Program – Standard Program

Event	Visa Action/Fee
Merchant Outlet meets or exceeds the Dispute activity thresholds specified in *Section 10.4.3.1, Visa Dispute Monitoring Program (VDMP)*, in months 1-4 (month 1 = initial notification).	• Workout Period[1] • No fee
Merchant Outlet meets or exceeds the Dispute activity thresholds specified in *Section 10.4.3.1, Visa Dispute Monitoring Program (VDMP)*, in months 5-9.	• A fee is assessed to the Acquirer, as specified in the applicable Fee Schedule, per Dispute[2] for every month the Merchant meets or exceeds the program thresholds.[3]
Merchant Outlet meets or exceeds the Dispute	• A fee is assessed to the Acquirer, as specified in

Table 12-11: Fees for Visa Dispute Monitoring Program – Standard Program (continued)

Event	Visa Action/Fee
activity thresholds specified in *Section 10.4.3.1, Visa Dispute Monitoring Program (VDMP)*, beyond month 9.	the applicable Fee Schedule, per Dispute[3] for every month the Merchant meets or exceeds the program thresholds.[3] • The Acquirer is eligible for a review fee, as specified in the applicable Fee Schedule. • Visa may initiate Merchant disqualification processes against a Merchant Outlet and/or its principals.

[1] The Workout Period does not apply to High-Risk Merchants or High-Brand Risk Merchants.

[2] VDMP non-compliance assessments and program fees apply to domestic and international Disputes for all the following: AP Region (Australia), Canada Region, Europe Region (Germany, United Kingdom), LAC Region (Brazil), and US Region. Visa may modify this list of markets. For all other markets, VDMP non-compliance assessments and program fees apply to only international Disputes.

[3] In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Visa may allocate a portion of this fee to the Issuer via a funds disbursement. Visa reserves the right to withhold or revoke funds disbursement from Issuers whose activities or lack of risk controls create a disproportionate volume of Disputes.

Table 12-12: Fees for Visa Dispute Monitoring Program – High-Risk Program

Event	Visa Action/Fee
Merchant Outlet meets or exceeds the Dispute activity thresholds specified in *Section 10.4.3.1, Visa Dispute Monitoring Program (VDMP)*, in months 1-6.	• A fee is assessed to the Acquirer, as specified in the applicable Fee Schedule, per Dispute[1] for every month the Merchant meets or exceeds the program thresholds.[2]
Merchant Outlet meets or exceeds the Dispute activity thresholds specified in *Section 10.4.3.1, Visa Dispute Monitoring Program (VDMP)*, beyond month 6.	• A fee is assessed to the Acquirer, as specified in the applicable Fee Schedule, per Dispute[1] for every month the Merchant meets or exceeds the program thresholds.[1] • The Acquirer is eligible for a review fee, as specified in the applicable Fee Schedule.
Merchant Outlet meets or exceeds the Dispute activity thresholds specified in *Section 10.4.3.1, Visa Dispute Monitoring Program (VDMP)*, beyond month 11.	• A fee is assessed to the Acquirer, as specified in the applicable Fee Schedule, per Dispute[1] for every month the Merchant meets or exceeds the program thresholds.[2]

Table 12-12: Fees for Visa Dispute Monitoring Program – High-Risk Program (continued)

Event	Visa Action/Fee
	• The Acquirer is eligible for a review fee, as specified in the applicable Fee Schedule. • Visa may initiate Merchant disqualification processes against a Merchant Outlet and/or its principals.
[1] VDMP non-compliance assessments and program fees apply to domestic and international Disputes for all the following: AP Region (Australia), Canada Region, Europe Region (Germany, United Kingdom), LAC Region (Brazil), and US Region. Visa may modify this list of markets. For all other markets, VDMP non-compliance assessments and program fees apply to only international Disputes.	
[2] In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Visa may allocate a portion of this fee to the Issuer via a funds disbursement. Visa reserves the right to withhold or revoke funds disbursement from Issuers whose activities or lack of risk controls create a disproportionate volume of Disputes.	

Non-compliance assessments and fees for Disputes activity under the VDMP standard program or VDMP high-risk program may continue to be assessed to the Acquirer:

• For all Trailing Dispute Activity that occurs up to 120 calendar days after Transaction processing has ceased

• Equivalent to the non-compliance assessments and fees being imposed on the Acquirer at the time Transaction processing ceased

Visa may assess, suspend, or waive VDMP fees and/or non-compliance assessments, in whole or in part, to accommodate unique or extenuating circumstances. The fees and/or non-compliance assessments will no longer be assessed to the Acquirer once the Merchant has met acceptable performance levels. However, fees and/or non-compliance assessments may continue to be assessed, or a Merchant may be prohibited from participating in the Visa Program, if Visa determines that the Merchant or Acquirer is causing undue economic hardship or harm to the goodwill of the Visa system as a result of high Dispute volumes.

ID# 0029291	Edition: Apr 2020	Last Updated: Oct 2019

12.6.5.2   Visa Dispute Monitoring Program (VDMP) – Data Quality Non-Compliance Assessments

Effective through 17 April 2020 If Visa determines that an Acquirer or its Merchant changed, modified, or altered the Merchant name, Merchant data, or Merchant performance in any way to circumvent the Visa Dispute Monitoring Program (VDMP), Visa may impose a non-compliance

assessment of up to USD 25,000 (or local currency equivalent) per Merchant Outlet, per month, to the Acquirer.

ID# 0029292	Edition: Apr 2020	Last Updated: Apr 2020

12.6.6   High-Risk/High-Brand Risk Acquirer Non-Compliance Assessments

12.6.6.1   High-Brand Risk Acquirer Registration Non-Compliance

If Visa determines that an Acquirer has failed to comply with the registration requirements specified in *Section 1.10.5.1, High-Brand Risk Acquirer Requirements,* Visa may impose a non-compliance assessment of USD 50,000 or, in the Europe Region, EUR 50,000 to the Acquirer per calendar month of non-compliance. Continued non-compliance may result in Visa prohibiting that Acquirer from acquiring High-Brand Risk Merchants or Electronic Commerce Merchants.

ID# 0026381	Edition: Apr 2020	Last Updated: Apr 2020

12.6.7   Fraud Monitoring and Reporting Non-Compliance Assessments

12.6.7.1   Visa Fraud Monitoring Program (VFMP) Non-Compliance Assessments

Visa assesses non-compliance assessments to the Acquirer of a Merchant Outlet identified in the Visa Fraud Monitoring Program (VFMP) high-risk program, as specified in *Section 10.4.5.2, Visa Fraud Monitoring Program (VFMP) Timelines*.

Table 12-13: Non-Compliance Assessments for VFMP – High-Risk Program

Month	Non-Compliance Assessment
Month 1 – 3	USD 10,000 per month
Month 4 – 6	USD 25,000 per month
Month 7 – 9	USD 50,000 per month
Month 10 – 12 (and, in the Europe Region, subsequent months)	USD 75,000 per month

Visa may assess, suspend, or waive VFMP non-compliance assessments, in whole or in part, to accommodate unique or extenuating circumstances. The non-compliance assessments will no longer be assessed to the Acquirer once its Merchant has met acceptable performance levels. However, non-compliance assessments may continue to be assessed, or a Merchant may be prohibited from participating in the Visa Program, if Visa determines that the Merchant or Acquirer

is causing undue economic hardship or harm to the goodwill of the Visa system as a result of high Fraud Activity volumes.

ID# 0029294	Edition: Apr 2020 | Last Updated: Oct 2018

12.6.7.2   Visa Fraud Monitoring Program (VFMP) – Data Quality Non-Compliance Assessments

Effective through 17 April 2020 If Visa determines that an Acquirer or its Merchant changed, modified, or altered the Merchant name or Merchant data in any way to circumvent the Visa Fraud Monitoring Program (VFMP), Visa may impose a non-compliance assessment of USD 10,000[1] per Merchant Outlet, per month, to the Acquirer.

[1] In the Europe Region: Or local currency equivalent

ID# 0029295	Edition: Apr 2020 | Last Updated: Apr 2020

12.6.7.5   Non-Compliance Assessments for Failure to Report Fraud – LAC Region

Effective through 17 April 2020 In the LAC Region: An Issuer that does not comply with the Fraud Reporting Program's requirements, as determined by the third or higher consecutive onsite audit, will be subject to a quarterly non-compliance assessment of USD 10,000 until found compliant by the Visa remote monitoring system and validated by an onsite audit.

ID# 0007267	Edition: Apr 2020 | Last Updated: Apr 2020

12.6.8   Terminated Merchant Non-Compliance Assessments

12.6.8.1   Terminated Merchant Non-Compliance Assessments – Canada Region

Effective through 17 April 2020 In the Canada Region: If an Acquirer fails to comply with *Section 10.11.2.3, Common Terminated Merchant Database Requirements – Canada Region,* Visa may assess a non-compliance assessment of CAD 2,500 per violation.

ID# 0007381	Edition: Apr 2020 | Last Updated: Apr 2020

12.6.9   Global Brand Protection Program Non-Compliance Assessments

12.6.9.2   Global Brand Protection Program Data Quality Non-Compliance Assessments

Effective through 17 April 2020 If Visa determines that an Acquirer or its Merchant changed, modified, or altered the Merchant name or Merchant data in any way to circumvent the Global Brand Protection Program, Visa may impose a non-compliance assessment of USD 10,000 or, in the Europe Region, EUR 10,000 per Merchant, per month, to the Acquirer.

ID# 0028286	Edition: Apr 2020 | Last Updated: Apr 2020

12.6.10   Corporate Risk Reduction Non-Compliance Assessments

12.6.10.1   Acquirer Responsibility for Merchants Non-Compliance Assessments – US Region

Effective through 17 April 2020 In the US Region: An Acquirer that fails to comply with the requirements of *Section 1.1.1.15, Visa U.S.A., Inc. Member Responsibilities – US Region*, is subject to a non-compliance assessment of X, termination of its membership, or both.

ID# 0008114	Edition: Apr 2020 | Last Updated: Apr 2020

12.6.11   Merchant Agreement with Prohibited Merchant Non-Compliance Assessments – US Region

12.6.11.1   Non-Compliance Assessments for Merchant Agreement with Prohibited Merchant – US Region

Effective through 17 April 2020 In the US Region: Visa imposes a non-compliance assessment to an Acquirer that enters into a Merchant Agreement with a Merchant, or known principals of a Merchant, that Visa has prohibited from participating in the Visa or Visa Electron Program, as follows:

Table 12-14: Acquirer Non-Compliance Assessments for Merchant Agreement with a Prohibited Merchant – US Region

Violation	Non-Compliance Assessment
First violation in a 5-year period	USD 10,000

Table 12-14: Acquirer Non-Compliance Assessments for Merchant Agreement with a Prohibited Merchant – US Region (continued)

Violation	Non-Compliance Assessment
Second violation in a 5-year period	USD 20,000
Third violation in a 5-year period	USD 50,000
4 or more violations in a 5-year period	At the discretion of Visa

Effective through 17 April 2020 Visa imposes an additional non-compliance assessment of USD 10,000 for each 30-calendar-day period, or portion thereof, during which the Acquirer fails to terminate the Merchant Agreement.

ID# 0007118	Edition: Apr 2020	Last Updated: Apr 2020

12.6.13   Non-Compliance Assessments Related to Agents

12.6.13.1 VisaNet Processor Non-Compliance Assessments

A Member using a VisaNet Processor that fails to comply with the Visa Rules and Visa Charter Documents is subject to non-compliance assessments, as specified in *Section 1.12.2.2, General Non-Compliance Assessment Schedules*. The combined liability of all Members for a VisaNet Processor's failure to comply must not be more than the non-compliance assessment amount for the violation involved.

Visa may impose non-compliance assessments resulting from the activities of a Member performing services on behalf of another Member to both the:

- Performing Member
- Member for which the services are performed

The total paid by both Members must not be more than the non-compliance assessment amount for the violation involved.

Visa may impose non-compliance assessments whether a Member or non-Member is performing services on behalf of another Member. If a Member acts as a VisaNet Processor for another Member, it is considered a single entity with that other Member in determining repetitive violations.

ID# 0025886	Edition: Apr 2020	Last Updated: Oct 2014

12.6.13.2 Third Party Agent Non-Compliance Assessments

Visa imposes non-compliance assessments to a Member that fails to comply with the requirements for use of Third Party Agents. A Member is subject to non-compliance assessments for the failure of its Third Party Agents to comply with the substance of Third Party Agent requirements, including non-payment of non-compliance assessments to Visa.

A Member that fails to comply with Third Party Agent requirements is subject to a non-compliance assessment, as follows:

Table 12-15: Non-Compliance Assessments Related to Third Party Agents

Violation	Non-Compliance Assessment
First occurrence	USD 10,000
Second occurrence in a rolling 60-month period	USD 25,000
Third occurrence in a rolling 60-month period	USD 50,000
Four or more occurrences in a rolling 60-month period	USD 100,000

For repeated violations in a rolling 60-month period, Visa may impose non-compliance assessments in addition to those specified in *Table 12-15, Non-Compliance Assessments Related to Third Party Agents,* at Visa discretion. Non-compliance assessments are cumulative.

ID# 0025901   **Edition: Apr 2020 | Last Updated: Oct 2019**

12.7   Fees – General

12.7.1   Global Compromised Account Recovery (GCAR) Fees

12.7.1.1   Global Compromised Account Recovery (GCAR) Fees – AP, Canada, CEMEA, LAC, and US Regions

In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: Visa will collect from the Acquirer through the Global Member Billing System either or both:

- A Global Compromised Account Recovery appeal fee
- A Global Compromised Account Recovery program non-cooperation analysis fee if the Acquirer, its Merchant, Acquirer processor, service provider, or other entity used by the Acquirer, its

Merchant, or ATM involved in processing Visa-branded Transactions refuses to allow a forensic investigation

ID# 0026568   Edition: Apr 2020 | Last Updated: Apr 2018

12.8   Member-to-Member Fees

12.8.2   Automated Clearing House Service

12.8.2.1   Automated Clearing House Collections Made in Error – US Region

In the US Region: Visa is not liable for automated clearing house collections made in error, except through intentional misconduct.

ID# 0007883   Edition: Apr 2020 | Last Updated: Oct 2014

12.8.2.2   Automated Clearing House Service Authorization Agreement – US Region

In the US Region: Visa will provide a Member or VisaNet Processor with an automated clearing house authorization agreement for Fee Collection Transactions and Funds Disbursement Transactions. This agreement must be signed and returned to Visa before the initiation of any automated clearing house transaction.

The signed agreement remains valid for all Fee Collection Transactions and Funds Disbursement Transactions until the Member or VisaNet Processor notifies Visa of either:

- Its replacement by a new agreement
- Revocation of the agreement because the Member or VisaNet Processor was terminated

ID# 0007974   Edition: Apr 2020 | Last Updated: Oct 2014

12.8.2.3   Automated Clearing House Service Requirements – US Region

In the US Region: Upon Visa request, a Member or VisaNet Processor must provide all of the following, for the purpose of collecting fees and disbursing funds through the automated clearing house service:

- Valid automated clearing house transit/routing number
- Associated financial institution depository account number
- Signed automated clearing house authorization agreement

If any account information (such as the account number or financial institution) changes, the Member or VisaNet Processor must both:

- Notify Visa at least 10 calendar days before the effective date of the change

- Submit a new automated clearing house authorization agreement with the change

ID# 0008067	Edition: Apr 2020	Last Updated: Oct 2014

12.8.2.4   Automated Clearing House Service Requirements for Principal-Type or Associate-Type Members – US Region

In the US Region: Upon Visa request, a Principal-type or Associate-type Member or an applicant for Principal-type or Associate-type membership must comply with *Section 12.8.2.3, Automated Clearing House Service Requirements – US Region,* for the purpose of collecting fees and disbursing funds through the automated clearing house service.

ID# 0007885	Edition: Apr 2020	Last Updated: Oct 2014

12.8.2.5   Initial Service Fee Collections through Automated Clearing House Service – US Region

In the US Region: Visa may collect initial service fees through the automated clearing house service from all new US Principal-type and Associate-type Members, as specified in the Visa Charter Documents.

ID# 0007884	Edition: Apr 2020	Last Updated: Oct 2014

12.8.2.6   Non-Use of Automated Clearing House Service – US Region

In the US Region: A Member or VisaNet Processor that is required to use the automated clearing house service may be required to reimburse Visa for any expense incurred for processing any payment made by a means other than the automated clearing house service.

ID# 0007882	Edition: Apr 2020	Last Updated: Oct 2014

12.8.2.7   Rejection of Automated Clearing House Transactions – US Region

In the US Region: Visa may require a same-day wire transfer, or initiate a Fee Collection Transaction through VisaNet, if a valid automated clearing house transaction is rejected or cannot be initiated for any reason, including:

- A Member did not comply with *Section 12.8.2.3, Automated Clearing House Service Requirements – US Region*
- Existing automated clearing house authorization agreement was revoked before a replacement authorization agreement took effect

ID# 0007881	Edition: Apr 2020	Last Updated: Oct 2014

12.8.3   Member-to-Member Fee Collection and Funds Disbursement

12.8.3.2   Fee Collection Time Limit

Unless otherwise specified, a Member must collect fees or disburse funds within 180 calendar days from the related event.

In the US Region: Unless otherwise specified, a Member must collect fees or disburse funds for a Domestic Transaction within 45 calendar days from the related event.

ID# 0003007	Edition: Apr 2020	Last Updated: Oct 2014

12.8.3.4   Resubmission of Returned Fee Collection

A Member may resubmit a returned Fee Collection Transaction for any of the following reasons:

- Information or documentation supporting the Fee Collection Transaction was not received
- Amount of the original Fee Collection Transaction was inaccurate
- Original Fee Collection Transaction was correct, but receiving Member returned it improperly

A Member resubmitting a returned Fee Collection Transaction must either:

- Make the resubmission within 30 calendar days from the date the Receiving Member returned the original Fee Collection Transaction
- In the US Region: Make the resubmission within 45 calendar days from the Central Processing Date of the returned Fee Collection Transaction

If the Fee Collection Transaction was returned because of missing information or documentation, the resubmission must contain the applicable information or documentation.

In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing*.

In the US Region: A Member must not resubmit a Fee Collection Transaction for Recovered Card handling fee/reward (reason code 0150) or recovery of Retrieval Request fees (reason code 0170).

ID# 0027791	Edition: Apr 2020 | Last Updated: Oct 2016

12.8.3.5   Limits of Fee Collection Returns

In no case may there be a third submission, return, or rejection of a Fee Collection Transaction through VisaNet. A Member that receives a third submission or return of a Fee Collection Transaction may pursue Compliance.

In the US Region: A Member must not submit an outstanding Fee Collection Transaction for Compliance for the following disputes, which must be settled directly between the Members involved and are not subject to Compliance procedures:

- Reason Code 0240 (Good Faith Collection Letter Settlement Funds Disbursement)
- Reason Code 0350 (Interchange Reimbursement Fee pre-Compliance Settlement Funds Disbursement)

ID# 0008059	Edition: Apr 2020 | Last Updated: Oct 2014

12.8.3.6   Member Fee Collection and Funds Disbursement Limitations

A Member must not use a Fee Collection Transaction for funds disbursement other than those listed in *Section X* and *Section 12.8.3.4, Resubmission of Returned Fee Collection.*

ID# 0003006	Edition: Apr 2020 | Last Updated: Oct 2014

12.8.3.7   Fee Collection/Funds Disbursement Process – US Region

In the US Region: When a Member or its Authorizing Processor collects fees or disburses funds as allowed through VisaNet, it must use transaction code 10 (Fee Collection Transaction) or transaction code 20 (Funds Disbursement Transaction).

No other use of the Fee Collection Transaction/Funds Disbursement Transaction process is permitted.

ID# 0003152	Edition: Apr 2020 | Last Updated: Oct 2014

12.8.4   Incentive Fulfillment Fees

12.8.4.1   Retrieval Request Fee Recovery

An Issuer may recover fees for Retrieval Requests for any of the following reasons:

- Acquirer did not properly supply the requested Transaction Receipt

- Request resulted from an incorrect Merchant description or a zero-filled or incorrect Transaction Date in the VisaNet transmission

- In the US Region: For a Domestic Transaction, both:

    – Requested copy was illegible

    – Acquirer did not properly supply the required Healthcare Auto-Substantiation Transaction detail

ID# 0003345	Edition: Apr 2020 | Last Updated: Apr 2018

12.8.5   Investigative Services Fees

12.8.5.1   Member Investigative Services Fee

A Member that requests investigative services from another Member must pay an investigative service fee, as specified in the applicable Fee Schedule.

A Member that performs investigative services for another Member must prepare an itemized statement for the Member requesting the services.

ID# 0008484	Edition: Apr 2020 | Last Updated: Oct 2014

12.8.6   Rewards for Recovered Cards

12.8.6.1   Recovered Card Rewards

An Acquirer must ensure that the minimum reward is paid to a Merchant that recovered a Visa Card or a Visa Electron Card, as specified in the applicable Fee Schedule.

If an Acquirer pays rewards to its tellers for the recovery of Visa Cards or Visa Electron Cards, it may collect the reward amount from the Issuer, as specified in the applicable Fee Schedule.

An Acquirer is not required to pay a reward, and an Issuer is not required to reimburse the Acquirer, for a Card that is any of the following:

- Expired

- Recovered at an ATM or Unattended Cardholder-Activated Terminal

- Inadvertently left at a Merchant Outlet

- A Non-Reloadable Prepaid Card recovered without a Pickup Response or a request from the Issuer

In the AP Region (Australia): An Issuer is not required to reimburse a reward paid by an Australia Acquirer to a person who is not a Merchant or a staff member of a Merchant (for example: law enforcement personnel, Acquirer employee).

In the US Region: If a recovered Card was retained by a law enforcement agency, the Acquirer must pay the reward upon receipt of a legible copy of the front and back of the recovered Card.

An Issuer must pay a reward for a recovered Visa Card or Visa Electron Card.

ID# 0001786	Edition: Apr 2020 | Last Updated: Apr 2019

12.8.6.2   Acquirer Recovered Card Handling and Reward Collection – US Region

In the US Region: If an Acquirer has paid a reward for a recovered Card, the Acquirer may collect the reward in a Fee Collection Transaction. Before entering the fee collection into Interchange, the Acquirer must notify the Issuer through Visa Resolve Online that the Card was recovered and specify the amount of the reward paid.

ID# 0008066	Edition: Apr 2020 | Last Updated: Apr 2017

12.9   Other Non-Compliance Assessments

12.9.1   Willful Violations – Europe Region

12.9.1.1   Willful Violation Non-Compliance Assessments – Europe Region

Effective through 24 January 2020 In the Europe Region: A Member that is found to have willfully violated the Visa Rules, as specified in *Section 1.12.2.8, Willful or Significant Violations Schedules,* is subject to a non-compliance assessment, as follows:

Table 12-16: Non-Compliance Assessments for Willful Violations of the Visa Rules – Europe Region

Violation	Non-Compliance Assessment
First violation of regulation	Warning letter with specific date for correction and EUR 50,000 non-compliance assessment (payment of the non-compliance assessment shall be suspended until end date for correction)
Second violation of the same regulation in a 12-month period after notification of first violation	EUR 100,000
Monthly increase thereafter for non-correction of	EUR 150,000 above previous month's total non-

Visa Product and Service Rules

12 Fees and Non-Compliance Assessments

Visa Core Rules and Visa Product and Service Rules

Table 12-16: Non-Compliance Assessments for Willful Violations of the Visa Rules – Europe Region (continued)

Violation	Non-Compliance Assessment
same violation	compliance assessments. For example, month 3=EUR 300,000; month 4=EUR 450,000 and so forth
Eight or more violations of the same regulation in a 12-month period after notification of first violation	Visa discretion
If the 12-month period is not violation-free and the non-compliance assessments total EUR 250,000 or more	Additional non-compliance assessment equal to all non-compliance assessments levied during that 12-month period

ID# 0029683   **Edition: Apr 2020 | Last Updated: Oct 2019**

VISA

Part 3:
Appendices

Appendix A

Visa Supplemental Requirements

Visa Supplemental Requirements (Enforceable Documents and Websites)

Visa Supplemental Requirements List

Visa Supplemental Requirements

Title	Applicable in Visa Region:
3-D Secure and Visa Secure	
3-D Secure Functional Requirements – Access Control Server	All
3-D Secure Functional Requirements – Merchant Server Plug-in	All
3-D Secure Protocol Specification Core Functions	All
3-D Secure U.S. Region Supplemental Functional Requirements – Access Control Server	US
Visa Secure Program Guide	All
Acceptance	
AVS ZIP Requirements for US AFD Merchants in High-Fraud Geographies	US
DCC Guide	All
Transaction Acceptance Device Requirements	All
Visa Merchant Data Standards Manual	All
Brand	
Visa Product Brand Standards	All
Card / Payment Device Technology	
EMV Contactless Specification for Payment Systems Book C-3	Europe
EMV Integrated Circuit Card Specifications for Payment Systems (EMV)	All

Appendices

Appendix A

Visa Core Rules and Visa Product and Service Rules

Title	Applicable in Visa Region:
Global Chip Fallback Monitoring Program Guide	All
Visa Canada Debit Card – Technical Specifications	Canada
Visa Chip Security Program – Security Testing Process	All
Visa Cloud-Based Payments Contactless Specifications	All
Visa Cloud-Based Payments Program Minimum Requirements and Guidelines	All
Visa Contactless Payment Specification	All
Visa Europe EMV Application Selection Requirements and Recommendations	Europe
Visa Europe Contactless Terminal Requirements and Implementation Guide	Europe
Visa Integrated Circuit Card Specification (VIS)	All
Visa Mobile Contactless Payment Specification (VMCPS)	All
Visa Mobile Gateway Issuer Update Functional Specification	All
Visa Mobile Gateway Issuer Update Protocol Specification	All
Visa Mobile Gateway Logical and Physical Security Requirements	All
Visa Mobile Gateway Secure Channel Functional Specification	All
Visa Mobile Gateway Secure Channel Protocol Specification	All
Visa QR Code Payment Specification (VQRPS)	AP
Visa Smart Debit/Credit Personalization Requirements for U.S. Implementations	US
Visa Smart Debit/Credit System Technical Manual	All
Encoding and PINs	
Payment Technology Standards Manual	All
Fee Schedules	
Visa Asia Pacific Fee Schedule	AP
Visa Canada Fee Schedule	Canada

Appendices

Appendix A

Visa Core Rules and Visa Product and Service Rules

Title	Applicable in Visa Region:
Visa CEMEA Fee Schedule	CEMEA
Visa Europe Fee Schedule	Europe
Visa LAC Fee Schedule	LAC
Visa U.S.A. Fee Schedule	US
Interchange Reimbursement Fees (IRF)	
AP Intraregional IRF Guide and AP Domestic IRF Guides, as applicable	AP
CEMEA Intraregional IRF Guide and CEMEA Domestic IRF Guides, as applicable	CEMEA
Europe Region Intraregional IRF Guide and Europe Domestic IRF Guides, as applicable	Europe
Interchange Reimbursement Fee Compliance Process Guide	All
Interregional Interchange Guide	All
LAC Intraregional IRF Guide and LAC Domestic IRF Guides, as applicable	LAC
US Interchange Reimbursement Fee Rate Qualification Guide	US
Visa Canada Interchange Guide	Canada
Visa Government and Education Payment Program Guide	US
Visa Government-to-Government (G2G) Program Guide	US
Visa U.S. Debt Repayment Incentive Interchange Program Guide	US
Visa U.S.A. Interchange Reimbursement Fees	US
Visa Utility Interchange Reimbursement Fee Program Guide	US
Licensing and BINs	
Product BIN Assignment Matrix – AP Region	AP
Product BIN Assignment Matrix – Canada Region	Canada
Product BIN Assignment Matrix – CEMEA Region	CEMEA

Appendices

Appendix A

Visa Core Rules and Visa Product and Service Rules

Title	Applicable in Visa Region:
Product BIN Assignment Matrix – Europe Region	Europe
Product BIN Assignment Matrix – LAC Region	LAC
Product BIN Assignment Matrix – US Region	US
Payment Card Industry Security Standards Council (PCI SSC)	
Payment Application Data Security Standard (PA-DSS)	All
Payment Card Industry 3-D Secure (PCI 3DS) Security Requirements and Assessment Procedures for EMV 3-D Secure Core Components: ACS, DS, and 3DS Server	All
Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements	All
Payment Card Industry (PCI) Card Production and Provisioning – Physical Security Requirements	All
Payment Card Industry Data Security Standard (PCI DSS)	All
Payment Card Industry (PCI) PIN Security Requirements	All
Payment Card Industry (PCI) PIN Transaction Security (PTS) – Point of Interaction (POI) Modular Security Requirements	All
Payment Card Industry (PCI) POS PIN Entry Device Security Requirements	Europe
Payment Card Industry (PCI) P2PE Solution Requirements and Testing Procedures	Europe
Products and Services	
Accelerated Connection Platform Acquirer Merchant Activation Guide	All, where available
Accelerated Connection Platform Client Implementation Guide	All, where available
Data Framework for Visa Services – Europe Region	Europe
Data Transfer Framework – Europe Region	Europe
PSD2 Strong Customer Authentication for Remote Electronic Transactions – European Economic Area	Europe

Appendix A

Visa Core Rules and Visa Product and Service Rules

Title	Applicable in Visa Region:
V PAY Card and Acceptance Device Technical Specifications	Europe
Visa Delegated Authentication Implementation Guide	Europe
Visa Digital Commerce Program Data Privacy and Security Terms and Role Requirements	All, where available
Visa Digital Solutions API Reference Guide	All, where available
Visa Europe Commercial Program Guide	Europe
Visa Mobile Prepaid Implementation Guide	All, where available
Visa Multinational Program Guide	All
Visa Ready Program for VDCP Digital Terminal Qualification and Solution Approval Process Guide	All, where available
Visa ReadyLink Service Description and Implementation Guidelines	US
Visa Secure Remote Commerce Digital Acceptance Gateway API Reference	All, where available
Visa Secure Remote Commerce Digital Acceptance Gateway Implementation Guide	All, where available
Visa Secure Remote Commerce Digital Terminal Implementation Guide	All, where available
Visa Secure Remote Commerce SDK Reference Guide	All, where available
Visa Token Service e-Commerce/Card-on-File Implementation Guide for Token Requestors	All, where available
Visa Settlement Match (VSM) Implementation Guide	All, where available[1]
Visa Trusted Listing Implementation Guide	Europe
Risk	
Account Information Security (AIS) Program Guide	All
Credit Settlement Risk Mitigation Structure for Deferred Transactions in Argentina	LAC Region (Argentina)
Fraud Reporting System (FRS) User's Guide	All

Appendices

Appendix A

Visa Core Rules and Visa Product and Service Rules

Title	Applicable in Visa Region:
Guidelines for Terminated Merchant Databases	Europe
Mobile P2M Push Payments Underwriting Standards	All
Third Party Agent Due Diligence Risk Standards	All
Visa Europe Card Vendor Programme Guide	Europe
Visa Global Acquirer Risk Standards	All
Visa Global Brand Protection Program Guide for Acquirers	All
Visa Global Compromised Account Recovery (GCAR) Guide	All except Europe
Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors	All
Visa PIN Security Program Guide	All
Visa Prepaid Issuer Risk Program Standards Guide	All
What To Do If Compromised	All except Europe
What To Do If Compromised: Visa Europe Data Compromise Procedures	Europe
Risk Products	
Card Recovery Bulletin Service (CRB) User's Guide	All
Prepaid Clearinghouse Service (PCS) Product Guide and Reporting Requirements	US
Visa Advanced ID Solutions (VAIS) User Guide and Best Practices	US
Settlement	
National Net Settlement Service Description	All[1]
Visa Settlement Funds Transfer Guide	All except Europe
Visa Europe Settlement Funds Transfer Guide	Europe
Transaction Processing	
Effective 18 April 2020 *Account Funding Transaction (AFT): Processing Guide*	All

Appendices

Appendix A
Visa Core Rules and Visa Product and Service Rules

Title	Applicable in Visa Region:
Visa Direct Original Credit Transaction (OCT) Global Implementation Guide	All
Visa Partial Authorization Service Description and Implementation Guide	All[1]
VisaNet Manuals	
BASE II Clearing Data Codes	All[1]
BASE II Clearing Edit Package Messages	All[1]
BASE II Clearing Edit Package Operations Guide	All[1]
BASE II Clearing Interchange Formats, TC 01 to TC 49	All[1]
BASE II Clearing Interchange Formats, TC 50 to TC 92	All[1]
BASE II Clearing PC Edit Package for Windows User's Guide	All[1]
BASE II Clearing Services	All[1]
BASE II Clearing System Overview	All[1]
BASE II Clearing VML Developer Handbook	All[1]
BASE II Clearing VML Formats	All[1]
V.I.P. System BASE I Processing Specifications	All[1]
V.I.P. System Overview	All[1]
V.I.P. System Services, Volume 1	All[1]
V.I.P. System Services, Volume 2	All[1]
V.I.P. System SMS ATM Processing Specifications (International)	All[1]
V.I.P. System SMS ATM Technical Specifications, Volume 1	All[1]
V.I.P. System SMS ATM Technical Specifications, Volume 2	All[1]
V.I.P. System SMS Interlink Client Implementation Guide	All[1]
V.I.P. System SMS Interlink Technical Specifications	All[1]
V.I.P. System SMS POS (Visa & Visa Electron) Processing Specifications (International)	All[1]

Title	Applicable in Visa Region:
V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1	All[1]
V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 2	All[1]
V.I.P. System SMS Processing Specifications (U.S.)	All[1]
VisaNet Authorization-Only Online Messages Technical Specifications, Volume 1	All[1]
VisaNet Authorization-Only Online Messages Technical Specifications, Volume 2	All[1]
VisaNet Settlement Service (VSS) User's Guide, Volume 1, Specifications	All[1]
VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports	All[1]

[1] In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region*, it must refer to *Visa Europe Operating Regulations – Processing.*

ID# 0028043   **Edition: Apr 2020 | Last Updated: Apr 2020**

VISA

Part 4:
Glossary

Glossary

0 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Term	Definition
0-9	
3-D Secure	A Visa-approved Authentication Method that is the global authentication standard for Electronic Commerce Transactions.
	ID# 0024200 — Edition: Apr 2020 | Last Updated: Apr 2010
3-D Secure Specification	A software protocol that enables secure processing of Transactions over the Internet and other networks. The 3-D Secure Specification includes: • *3-D Secure Protocol Specification Core Functions* • *3-D Secure Functional Requirements Access Control Server* • *3-D Secure Functional Requirements Merchant Server Plug-in* • In the US Region: *3-D Secure US Region Supplemental Functional Requirements – Access Control Server* • *EMV 3-D Secure Protocol and Core Functions Specification* • *EMV 3-D Secure SDK – Device Information* • *EMV 3-D Secure SDK Specification*
	ID# 0024203 — Edition: Apr 2020 | Last Updated: Apr 2018
A	
Acceptance Device	A Card-reading device managed by a Member or a Merchant for the purpose of completing a Visa Transaction.
	ID# 0029278 — Edition: Apr 2020 | Last Updated: Apr 2016
Access Fee	A fee assessed by an Acquirer to a Cardholder in connection with a Cash Disbursement or a Shared Deposit Transaction.
	ID# 0024207 — Edition: Apr 2020 | Last Updated: Apr 2019
Account Data Compromise Event	An event in which account data is put at risk.
	ID# 0026743 — Edition: Apr 2020 | Last Updated: Oct 2015

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Account Funding Transaction	A Transaction where funds are pulled from a Visa account and are subsequently used to fund another Visa or non-Visa account. ID# 0024213 Edition: Apr 2020 | Last Updated: Apr 2020
Account Information Security Program	A program managed by Visa that defines the standards of due care and enforcement for protecting sensitive Cardholder information and supports both: • *Payment Card Industry Data Security Standard (PCI DSS)* • *Payment Card Industry Payment Application Data Security Standard (PA-DSS)* ID# 0024215 Edition: Apr 2020 | Last Updated: Oct 2014
Account Level Processing	An optional service provided by Visa that enables an Issuer: • To manage select product-based services at the Account Number level instead of the BIN level • To dynamically move Card products up and down the product spectrum without having to change the associated Account Number ID# 0027308 Edition: Apr 2020 | Last Updated: Apr 2019
Account Number	An Issuer-assigned Payment Credential that identifies an account in order to post a Transaction. ID# 0024216 Edition: Apr 2020 | Last Updated: Apr 2020
Account Number Verification	A process by which a Member or its VisaNet Processor determines, using a currency unit of zero, if there is negative information on an Account Number in the Exception File for Transactions that do not require Authorization. ID# 0024217 Edition: Apr 2020 | Last Updated: Oct 2011
Account Range	The first 9 digits of a BIN, used to identify Issuers and products. ID# 0030610 Edition: Apr 2020 | Last Updated: Apr 2019
Account Verification	A message sent by an Acquirer to the Issuer, using a currency unit of zero, for confirmation that a Transaction can be completed using the Card. ID# 0029700 Edition: Apr 2020 | Last Updated: Oct 2017

Glossary	

Glossary

Visa Core Rules and Visa Product and Service Rules

Acquirer	A Member that signs a Merchant or Payment Facilitator, provides a Cash Disbursement to a Cardholder, or loads funds to a Prepaid Card, and directly or indirectly enters a Transaction into Interchange. In the Europe Region: A Member that either: • Enters into an agreement with a Merchant for the display of any of the Visa-Owned Marks and the acceptance of Visa products and services • Disburses currency to a Cardholder, except where "Acquirer" is otherwise defined for the Europe Region in the Visa Rules ID# 0024219 Edition: Apr 2020 | Last Updated: Apr 2020
Acquirer Confirmation Advice	A message sent from an Acquirer to an Issuer confirming the final Transaction Amount. ID# 0026794 Edition: Apr 2020 | Last Updated: Oct 2017
Acquirer Device Validation Toolkit (ADVT)	A set of cards or simulated cards and test scenarios used to validate new or upgraded EMV Chip-Reading Devices. ID# 0024222 Edition: Apr 2020 | Last Updated: Apr 2010
Acquirer Processor	A non-Member agent or processor that a Member has engaged to support its Visa acquiring business. ID# 0024225 Edition: Apr 2020 | Last Updated: Oct 2017
Acquirer Reference Number	An identification number included in a Clearing Record. ID# 0024226 Edition: Apr 2020 | Last Updated: Oct 2016
Acquiring Identifier	A 6-digit identifier licensed by Visa to an Acquirer and that is used to identify an Acquirer. ID# 0030646 Edition: Apr 2020 | Last Updated: Oct 2019
Acquiring Identifier Licensee	An Acquirer, or non-Member VisaNet Processor or Visa Scheme Processor, or non-Interlink Member Processor that is allocated responsibility by Visa for a specific Acquiring Identifier, as specified in the Visa Rules and applicable Visa Charter Documents. ID# 0030644 Edition: Apr 2020 | Last Updated: Oct 2019
Acquiring Identifier User	An Acquirer authorized to use an Acquiring Identifier licensed to its Sponsor, as specified in the Visa Rules.

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	ID# 0030645 Edition: Apr 2020 | Last Updated: Oct 2019
Acquisition	The purchase of a Member organization by another organization where the acquired Member's charter remains intact.
	ID# 0024229 Edition: Apr 2020 | Last Updated: Oct 2011
Address Verification Service	A VisaNet service through which a Merchant verifies a Cardholder's billing address.
	ID# 0024238 Edition: Apr 2020 | Last Updated: Oct 2017
Adjustment	A Single Message System message used to partially or fully negate or cancel a transaction that has been sent through Interchange in error.
	ID# 0024241 Edition: Apr 2020 | Last Updated: Apr 2010
Advanced Resolution Services, Inc. – US Region	A wholly-owned subsidiary of Visa U.S.A. that provides Members with services such as Advanced ID Solutions and Strategic Bankruptcy Solutions.
	ID# 0024245 Edition: Apr 2020 | Last Updated: Oct 2014
Advance Payment	**Effective 25 January 2020** A Transaction for the partial or full cost of goods or services that will be provided to the Cardholder at a later time.
	ID# 0030637 Edition: Apr 2020 | Last Updated: New
Affinity/Co-Brand	A program or partnership based on a contractual agreement between an Issuer and a Member or non-Member for the issuance of Cards bearing the Affinity/Co-Brand partner's Trade Name or Mark.
	ID# 0029280 Edition: Apr 2020 | Last Updated: Oct 2018
Agent	An entity that acts as a VisaNet Processor/Visa Scheme Processor, a Third Party Agent, or both.
	ID# 0025920 Edition: Apr 2020 | Last Updated: Apr 2020
Aggregated Transaction	A single Transaction that combines multiple purchases made by the same Cardholder on the same Payment Credential at the same Merchant during a defined time period and up to a defined amount.
	ID# 0024270 Edition: Apr 2020 | Last Updated: Apr 2020
Airline	A Merchant that transports passengers on an aircraft.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0024273 Edition: Apr 2020 | Last Updated: Apr 2016
Airline Authorizing Processor	A Visa-approved non-Member whose primary function is to provide reservation and Authorization services for Airline Transactions, or travel-related services that include the purchase of an Airline ticket.
	ID# 0024274 Edition: Apr 2020 | Last Updated: Oct 2014
Airline Ticket Identifier	A unique value (for example: carrier code or number, ticket serial number, transmission control number) of up to 13 characters that identifies the purchase of an Airline ticket.
	ID# 0024278 Edition: Apr 2020 | Last Updated: Oct 2015
Alert – Europe Region	A message sent by a Visa Alerts Service to a Cardholder by email, SMS (Short Message Service), or push notification.
	ID# 0029704 Edition: Apr 2020 | Last Updated: Oct 2016
Ancillary Purchase Transaction	The purchase of goods and services, other than a passenger ticket, completed at an Airline or a US passenger railway Merchant.
	ID# 0029155 Edition: Apr 2020 | Last Updated: Oct 2015
AP	Asia-Pacific.
	ID# 0024281 Edition: Apr 2020 | Last Updated: Apr 2010
Application Identifier	An EMV-compliant data label encoded on a Chip Card and loaded on a Chip Reading Device that is used to identify mutually supported payment applications.
	ID# 0029281 Edition: Apr 2020 | Last Updated: Oct 2015
Application Label – Europe Region	A name that identifies an application stored on a Card and that is used during application selection when no application preferred name is associated with that application.
	ID# 0029705 Edition: Apr 2020 | Last Updated: Oct 2016
Application Selection Flag – Canada Region	An EMV-compliant Canadian payment industry specification that allows an Issuer to control which payment applications contained in a Compliant Chip Card can process a Transaction at a POS or an ATM.
	ID# 0024284 Edition: Apr 2020 | Last Updated: Oct 2014
Application Transaction Counter	A counter within the application on a contact Chip or Contactless Card that tracks the number of times the Chip is read and that is used by the

<table>
<tr><td colspan="2" align="center">**Glossary**</td></tr>
</table>

	Issuer during the Authorization process.
	ID# 0024286 Edition: Apr 2020 | Last Updated: Apr 2018
Approval Response	An Authorization Response where the Transaction was approved.
	ID# 0024287 Edition: Apr 2020 | Last Updated: Apr 2010
Arbitration	A process where Visa determines financial liability between Members for Interchange Transactions that are presented and have completed the Dispute cycle.
	ID# 0024289 Edition: Apr 2020 | Last Updated: Apr 2018
Arbitration and Compliance Committee	A Visa committee that resolves certain disputes between Members that arise from Disputes or from violations of the Visa Rules.
	ID# 0024290 Edition: Apr 2020 | Last Updated: Apr 2018
Associate-Type Member	A Member of Visa that is an Associate with rights and responsibilities, as defined in the applicable Visa Charter Documents.
	ID# 0024293 Edition: Apr 2020 | Last Updated: Apr 2018
ATM Operator – US Region	An entity authorized by a Member or its Agent to originate a Transaction through the connection of an ATM to the Visa ATM Network and that displays the Visa acceptance Mark. An ATM Operator owns, operates, or leases ATMs that are connected to the Visa ATM Network and may either or both: • Receive revenue from the Interchange process or from fees assessed with Transactions • Manage cryptographic functions or stock ATMs with cash
	ID# 0024301 Edition: Apr 2020 | Last Updated: Oct 2015
Attempt Response	A message from a Visa Secure Issuer or Visa in response to an Authentication Request, indicating that the Issuer or Cardholder is not participating in Visa Secure.
	ID# 0024302 Edition: Apr 2020 | Last Updated: Apr 2019
Authentication	A cryptographic process that validates the identity and integrity of Chip data.
	ID# 0024303 Edition: Apr 2020 | Last Updated: Apr 2010
Authentication	A message from a Visa Secure Issuer in response to an Authentication

Confirmation	Request confirming Cardholder authentication.
	ID# 0024304 Edition: Apr 2020 | Last Updated: Apr 2019
Authentication Data	All Transaction-related data associated with a Visa Secure Authentication Request.
	ID# 0026423 Edition: Apr 2020 | Last Updated: Apr 2019
Authentication Denial	A message sent by a Visa Secure Issuer in response to an Authentication Request, that denies Cardholder authentication.
	ID# 0024306 Edition: Apr 2020 | Last Updated: Apr 2019
Authentication Mechanism	A Visa-approved method that validates a participant's identity in an Electronic Commerce Transaction. Authentication Mechanisms include, but are not limited to: • Password • Digital Certificate
	ID# 0024309 Edition: Apr 2020 | Last Updated: Apr 2010
Authentication Method	A Visa-approved protocol, such as Visa Secure, that meets the minimum standards for authenticating a Cardholder in an Electronic Commerce Transaction.
	ID# 0024310 Edition: Apr 2020 | Last Updated: Oct 2019
Authentication Record	A record of the Visa Secure authentication status from a Visa Secure Issuer in response to an Authentication Request.
	ID# 0024311 Edition: Apr 2020 | Last Updated: Apr 2019
Authentication Request	A request for Cardholder authentication from a Visa Secure Merchant.
	ID# 0024313 Edition: Apr 2020 | Last Updated: Apr 2019
Authentication Response	A response from a Visa Secure Issuer, or Visa on behalf of an Issuer, in response to an Authentication Request. Authentication Responses include: • Attempt Responses • Authentication Confirmations • Authentication Denials • Unable-to-Authenticate Responses

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	ID# 0026811 Edition: Apr 2020 | Last Updated: Apr 2019
Authorization	A process where an Issuer, a VisaNet Processor, Visa Scheme Processor, or Stand-In Processing approves a Transaction. This includes Offline Authorization.
	ID# 0024316 Edition: Apr 2020 | Last Updated: Oct 2018
Authorization and Settlement Match	An optional Visa service offered to Issuers in connection with Visa Purchasing Card Commercial Payables Transactions which allows Visa to edit for an exact match between the amount in the Authorization Request and the corresponding Clearing Record. The service applies only to Transactions conducted at a non-T&E Merchant or Lodging Merchant, as specified in the *Visa Settlement Match (VSM) Implementation Guide*
	In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing*.
	ID# 0026823 Edition: Apr 2020 | Last Updated: Oct 2016
Authorization Code	A code that an Issuer, its VisaNet Processor, a Visa Scheme Processor, or Stand-In Processing provides to indicate approval of a Transaction. The code is returned in the Authorization Response message and is usually recorded on the Transaction Receipt as proof of Authorization.
	ID# 0024317 Edition: Apr 2020 | Last Updated: Oct 2016
Authorization Preferred Visa Prepaid Card	A Prepaid Card that has a Service Code denoting "Online Authorization mandatory" encoded on the Magnetic Stripe.
	ID# 0024318 Edition: Apr 2020 | Last Updated: Apr 2020
Authorization Request	A Merchant or Acquirer request for an Authorization.
	ID# 0024319 Edition: Apr 2020 | Last Updated: Oct 2014
Authorization Request Cryptogram	An application Cryptogram generated by a Chip Card when requesting Online Authorization.
	ID# 0025502 Edition: Apr 2020 | Last Updated: Oct 2011
Authorization Response	An Issuer's reply to an Authorization Request or Account Number Verification that refers to the following types of Authorization Responses:

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	• Approval Response • Decline Response • Pickup Response ID# 0024321 Edition: Apr 2020 | Last Updated: Oct 2017
Authorization Reversal	A system message that cancels an Approval Response. ID# 0025601 Edition: Apr 2020 | Last Updated: Oct 2016
Authorizing Processor	A Member or its VisaNet Processor or Visa Scheme Processor that provides Authorization services for Merchants or other Members. In the US Region, this definition does not imply or confer membership rights as defined in the *Visa U.S.A. Inc. Certificate of Incorporation and By-Laws*, Article II. ID# 0024324 Edition: Apr 2020 | Last Updated: Oct 2016
Auto Rental Collision Damage Waiver	A Card feature that provides Cardholders with collision or loss damage insurance on car rental Transactions. ID# 0024453 Edition: Apr 2020 | Last Updated: Apr 2020
Automated Fuel Dispenser	An Unattended Cardholder-Activated Terminal that dispenses only fuel. An Automated Fuel Dispenser may also facilitate a Transaction originating from an application using a Stored Credential on a Cardholder device. ID# 0024328 Edition: Apr 2020 | Last Updated: Apr 2018
B	
Balance Inquiry	A Cardholder request for an account balance that is initiated at an ATM and processed as a separate, non-financial transaction. ID# 0024334 Edition: Apr 2020 | Last Updated: Oct 2014
Balance Inquiry Service	An ATM service that allows a Cardholder to check an account balance. ID# 0024335 Edition: Apr 2020 | Last Updated: Oct 2016
BASE I	A component of the V.I.P. System that provides Authorization-related services for Transactions that are subsequently cleared and settled through BASE II. ID# 0024343 Edition: Apr 2020 | Last Updated: Apr 2011

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

BASE II	A VisaNet system that provides deferred Clearing and Settlement services to Members.
	ID# 0024341 Edition: Apr 2020 | Last Updated: Apr 2010
Bill Payment Transaction	A Transaction that results from an agreement between a Cardholder and a Merchant made in advance of the Cardholder being billed for goods or services conducted within an ongoing service cycle. Transactions may occur monthly or on a periodic basis. Such Transactions include: • Single payments initiated by the Cardholder in a Face-to-Face Environment, in a Card-Absent Environment, or at an ATM • Recurring Transactions • Installment Transactions
	ID# 0024350 Edition: Apr 2020 | Last Updated: Apr 2017
Billing Currency	The currency in which an Issuer bills and receives payment from a Cardholder for Transactions, or debits the associated Cardholder's account for Transactions.
	ID# 0024349 Edition: Apr 2020 | Last Updated: Oct 2016
BIN	Bank Identification Number. Either: • A 6-digit identifier assigned by ISO to Visa and then licensed by Visa to an Issuer before 22 April 2022 and that comprises the first 6 digits of an Account Number. • An 8-digit identifier assigned by ISO to Visa and then licensed by Visa to an Issuer and that comprises the first 8 digits of an Account Number.
	ID# 0024351 Edition: Apr 2020 | Last Updated: Oct 2019
BIN Attribute	Information that identifies the characteristics of a BIN and Visa products issued from that BIN. BIN Attributes include, but are not limited to, account funding source, account funding source subtype, product ID, Issuer name, Issuer country, and Issuer currency.
	ID# 0030648 Edition: Apr 2020 | Last Updated: New
BIN Licensee	An Issuer that is allocated responsibility by Visa for a specific BIN, as specified in the Visa Rules and applicable Visa Charter Documents.

	ID# 0024352	Edition: Apr 2020 | Last Updated: Oct 2019
BIN User	An Issuer authorized to use a BIN licensed to its Sponsor, as specified in the Visa Rules.	
	ID# 0025530	Edition: Apr 2020 | Last Updated: Oct 2019
Board of Directors	One of the following, as applicable: ● Visa Inc. Board of Directors ● Visa International Board of Directors ● Visa U.S.A. Board of Directors ● Visa Canada Board of Directors ● Visa Europe Board of Directors ● Visa International Servicios de Pago España, S.R.L.U. Board of Directors ● Visa Worldwide Board of Directors	
	ID# 0024354	Edition: Apr 2020 | Last Updated: Oct 2016
Branch	The office of a Member where Manual Cash Disbursements may be made and Cards may be issued excluding drive-through windows providing reduced customer services, in-store counters, or service centers that do not store cash on the premises.	
	ID# 0024355	Edition: Apr 2020 | Last Updated: Oct 2016
C		
Campus Card – US Region	A Debit Card or Prepaid Card issued to a student, staff member, or faculty member of an educational organization in the US Region that both: ● Bears the Visa Mark ● Includes one or more of the following applications: identification, building access, library access, or a proprietary closed-loop payment application for use only within a college or university system	
	ID# 0024358	Edition: Apr 2020 | Last Updated: Apr 2020
Card	A payment card, digital application, or other device or solution that provides access to a Payment Credential and that is capable of conducting a Transaction, is issued by an Issuer, and may bear one of	

	the Visa-Owned Marks.	
	ID# 0024365	Edition: Apr 2020 | Last Updated: Apr 2020
Card Linked Offers Service – Europe Region	A service provided by Visa that associates a commercial offer with a Card.	
	ID# 0030566	Edition: Apr 2020 | Last Updated: Apr 2018
Card Recovery Bulletin	A directory of blocked Account Numbers, intended for distribution to Merchants. It may take one of the following forms: • National Card Recovery Bulletin (a special edition that lists domestic Account Numbers in addition to other applicable listings) • National Card Recovery File • Regional Card Recovery File	
	ID# 0024390	Edition: Apr 2020 | Last Updated: Oct 2016
Card Verification Service	A service where a Card Verification Value in an Authorization Request is validated on behalf of an Issuer.	
	ID# 0024398	Edition: Apr 2020 | Last Updated: Oct 2016
Card Verification Value	A unique check value encoded on the Magnetic Stripe of a Card to validate Card information during the Authorization process. The Card Verification Value is calculated from the data encoded on the Magnetic Stripe using a secure cryptographic process.	
	ID# 0024399	Edition: Apr 2020 | Last Updated: Apr 2010
Card Verification Value 2	A unique check value generated using a secure cryptographic process that, when displayed, is displayed either statically or dynamically (referenced as dCVV2) on a Card or provided to a Virtual Account owner.	
	ID# 0024400	Edition: Apr 2020 | Last Updated: Apr 2020
Card-Absent Environment	An environment in which a Transaction is completed under both of the following conditions: • Cardholder is not present • Card is not present	
	ID# 0024362	Edition: Apr 2020 | Last Updated: Oct 2015

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Card-Present Environment	An environment in which a Transaction is completed under all of the following conditions:
	
	• Card is present
	
	• Cardholder is present at the Merchant Outlet
	
	• Transaction is completed by either:
	
	  – A representative of the Merchant or Acquirer
	
	  – The Cardholder directly at an Unattended Cardholder-Activated Terminal
	
	ID# 0024363 Edition: Apr 2020 | Last Updated: Apr 2018

Cardholder	An individual who is issued a Card. ID# 0024372 Edition: Apr 2020 | Last Updated: Apr 2020
Cardholder Authentication Verification Value (CAVV)	A unique value transmitted in response to an Authentication Request. ID# 0024375 Edition: Apr 2020 | Last Updated: Apr 2013
Cardholder Inquiry Service	A service that assists Cardholders in obtaining information about Visa products, their Visa accounts, and the benefits associated with their Cards. ID# 0024379 Edition: Apr 2020 | Last Updated: Apr 2020
Cardholder Maintenance File – US Region	A file containing Cardholder names, addresses, and account information provided to Visa and used for various account-related activities. ID# 0024380 Edition: Apr 2020 | Last Updated: Oct 2014
Cardholder Verification	The process of validating a Cardholder's identity through verification of the Cardholder's signature, PIN, Consumer Device Cardholder Verification Method (CDCVM), or other methods as required in the Visa Rules. ID# 0024381 Edition: Apr 2020 | Last Updated: Oct 2018
Cardholder Verification Limit – Europe Region	The Transaction amount for Contactless Transactions above which Cardholder Verification must be performed. ID# 0029706 Edition: Apr 2020 | Last Updated: Oct 2016
Cardholder Verification Method	A means of verifying that the person presenting a Card is the legitimate Cardholder.

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

	For a Chip Card, the hierarchy of preferences for verifying a Cardholder's identity is encoded within the Chip.
	ID# 0024382 _Edition: Apr 2020 | Last Updated: Oct 2015_
Cash Disbursement	Currency, including travelers cheques and excluding Cash-Back, provided to a Cardholder as follows: • As a Cash-Out • As a Manual Cash Disbursement • Through an ATM
	ID# 0024407 _Edition: Apr 2020 | Last Updated: Oct 2018_
Cash Disbursement Fee	A fee paid by an Issuer to an Acquirer for performing a Cash Disbursement.
	ID# 0024409 _Edition: Apr 2020 | Last Updated: Apr 2010_
Cash-Back	Cash obtained from a Merchant through use of a Card in conjunction with, and processed as, a Retail Transaction.
	ID# 0024406 _Edition: Apr 2020 | Last Updated: Apr 2020_
Cash-In	Cash deposited at a Merchant that supports Mobile Push Payment Transactions, for crediting a Payment Credential.
	ID# 0030582 _Edition: Apr 2020 | Last Updated: Apr 2020_
Cash-Out	Cash obtained by a Visa account holder from a Merchant that supports Mobile Push Payment Transactions.
	ID# 0030583 _Edition: Apr 2020 | Last Updated: Oct 2018_
CEMEA	Central and Eastern Europe, Middle East, and Africa.
	ID# 0024413 _Edition: Apr 2020 | Last Updated: Apr 2010_
Chargeback Reduction Service	A service that screens Presentments and Disputes and returns certain invalid items to the Acquirer or Issuer, as appropriate.
	ID# 0024429 _Edition: Apr 2020 | Last Updated: Apr 2018_
Cheque	A traveler's cheque that a Member has issued and that bears the Visa-Owned Marks.
	ID# 0024431 _Edition: Apr 2020 | Last Updated: Oct 2014_

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Chip	An electronic component designed to perform processing or memory functions that communicates with an Acceptance Device using a contact or Contactless interface and enables Visa Transaction processing or performs other Visa-approved functions . ID# 0024436 Edition: Apr 2020 | Last Updated: Oct 2015
Chip Specifications – Canada Region	All requirements set out in the EMV, VIS, VSDC, PCI, and Visa PIN Entry Device specifications. ID# 0024439 Edition: Apr 2020 | Last Updated: Oct 2014
Chip-initiated Transaction	An EMV-Compliant and VIS-Compliant Chip Card Transaction that is processed at a Chip-Reading Device using Full-Chip Data, and limited to Visa and Visa Electron Smart Payment applications, or EMV-Compliant and VIS-Compliant Plus applications. ID# 0024433 Edition: Apr 2020 | Last Updated: Apr 2020
Chip-Reading Device	An Acceptance Device capable of reading, communicating, and processing Transaction data from a Chip. ID# 0024435 Edition: Apr 2020 | Last Updated: Apr 2020
Clearing	All of the functions necessary to collect a Clearing Record from an Acquirer in the Transaction Currency and deliver it to the Issuer in the Billing Currency, or to reverse this transaction, or to process a Fee Collection Transaction. ID# 0024444 Edition: Apr 2020 | Last Updated: Apr 2010
Clearing Processor	A Member or its Visa-approved VisaNet Processor or Visa Scheme Processor that provides Clearing and/or Settlement services for Merchants or other Members. This definition does not imply or confer membership rights as defined in the *Visa International Certificate of Incorporation and By-Laws*, Article II, in the *Visa U.S.A. Inc. Certificate of Incorporation and By-Laws*, Article II, in the *Visa Worldwide Supplementary Operating Regulations* (for Asia-Pacific), Section 1, or in the *Visa International Servicios de Pago España, S.R.L.U. Supplementary Operating Regulations* (for Latin America & Caribbean), Section 1. ID# 0026051 Edition: Apr 2020 | Last Updated: Oct 2016
Clearing Record	A record of a Presentment, Dispute, Dispute Response, Acquirer-initiated pre-Arbitration, Reversal, or Adjustment in the format necessary to clear the Transaction.

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0024446 Edition: Apr 2020 | Last Updated: Apr 2018
Clearing Reversal – US Region	A VisaNet Transaction that negates a Transaction previously sent through BASE II or the Single Message System.
	ID# 0024447 Edition: Apr 2020 | Last Updated: Apr 2018
Client Contact Tool	A Client Directory module that contains Member contact information used by Visa for the delivery of critical corporate and operational email communications to Members.
	ID# 0030655 Edition: Apr 2020 | Last Updated: Oct 2019
Client Directory	An online Visa directory that contains contact information for Visa, Plus, and Interlink Members and processors and that is comprised of the Client Service Provider Directory module and the Client Contact Tool module.
	ID# 0030015 Edition: Apr 2020 | Last Updated: Oct 2019
Client Organization	A company or organization that sponsors a Visa Corporate Card or Visa Purchasing Card (including Visa Fleet Card in the US Region), or any other Visa Commercial Card program combining the functionality of these Cards, wherein Cards are provided to users for business-related purchases. Such companies or organizations may include public or private-sector companies, including sole proprietors.
	ID# 0026020 Edition: Apr 2020 | Last Updated: Apr 2020
Client Portfolio Management Self-Service Tools	A set of tools, available through Visa Online to Members, VisaNet Processors, and designated Agents, providing the ability to manage and support Visa profile information and associated programs and comprising the following: • Program Request Management (PRM) • Electronic Client Information Questionnaire (eCIQ) • Visa Client Support Application (VCSA)
	ID# 0026479 Edition: Apr 2020 | Last Updated: Apr 2018
Client Service Provider Directory	A Client Directory module that contains BID, BIN, Acquiring Identifier, service provider and/or Member information and is used for Member-to-Member communication and problem resolution.
	ID# 0030656 Edition: Apr 2020 | Last Updated: Oct 2019

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Closed Loop – Europe Region	An environment using a Visa Drive Card where the Acquirer and Issuer are the same.
	ID# 0029707 · Edition: Apr 2020 | Last Updated: Oct 2016
Collateral Material	Printed, broadcast, or other communications regarding an Affinity/Co-Brand partner's Trade Name or Mark. These may include, but are not limited to, solicitations, promotional materials, advertisements, statements, statement inserts, direct mail solicitations, and telemarketing operator scripts.
	ID# 0027362 · Edition: Apr 2020 | Last Updated: Oct 2015
Collection-Only	The reporting of data related to a Domestic Transaction that was processed outside of VisaNet and submitted only for informational purposes.
	ID# 0027828 · Edition: Apr 2020 | Last Updated: Oct 2014
Commercial Payables	An environment where a Visa Commercial Card Transaction occurs between business entities, generally through negotiated contractual agreements, or in response to the generation of an invoice requesting payment for goods or services.
	ID# 0026824 · Edition: Apr 2020 | Last Updated: Oct 2017
Compelling Evidence	Information or documentation provided by a Merchant or an Acquirer in a Dispute Response or pre-Arbitration that attempts to prove that the Cardholder participated in the Transaction, received goods or services, or otherwise benefited from the Transaction, as specified in *Section 11.5.2, Use of Compelling Evidence*. Compelling Evidence does not mandate that Visa, the Issuer, or any other entity conclude that the Cardholder participated in the Transaction, received goods or services, agreed to Dynamic Currency Conversion, or otherwise benefited from the Transaction.
	ID# 0027268 · Edition: Apr 2020 | Last Updated: Apr 2018
Competitive Credit Card Brand – US Region and US Territories	In the US Region, US Territory: Any brand of credit card or electronic credit payment form of a nationally accepted payment network other than Visa, including without limitation MasterCard, American Express, Discover, and PayPal.
	ID# 0027526 · Edition: Apr 2020 | Last Updated: Oct 2014
Competitive Credit Card Cost of Acceptance – US	In the US Region, US Territory: The Merchant's average Merchant Discount Rate applicable to transactions on a Competitive Credit Card

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

Region and US Territories	Brand at the Merchant for the preceding one or 12 months, at the Merchant's option. ID# 0027527 Edition: Apr 2020 | Last Updated: Oct 2014
Competitive Credit Card Product – US Region and US Territories	In the US Region, US Territory: Any product within a brand of credit card or electronic credit payment form of a nationally accepted payment network other than Visa, including without limitation MasterCard, American Express, Discover, and PayPal. ID# 0027528 Edition: Apr 2020 | Last Updated: Oct 2014
Competitive Credit Card Product Cost of Acceptance – US Region and US Territories	In the US Region, US Territory: The Merchant's average effective Merchant Discount Rate applicable to transactions on the Competitive Credit Card Product at the Merchant for the preceding one or 12 months, at the Merchant's option. ID# 0027529 Edition: Apr 2020 | Last Updated: Oct 2014
Completion Message	A Clearing Record that follows a preauthorization as part of Real-Time Clearing Processing. ID# 0024469 Edition: Apr 2020 | Last Updated: Oct 2014
Compliance	A process where Visa resolves disputes between Members arising from violations of the Visa Rules, when the requesting Member can certify that a financial loss has occurred or will occur for a specific amount, and no Dispute right is available. ID# 0024470 Edition: Apr 2020 | Last Updated: Apr 2018
Compliant Chip Card	A Chip Card that contains a Visa Smart Payment application capable of processing Full Data and that complies with Chip Specifications. ID# 0024471 Edition: Apr 2020 | Last Updated: Apr 2018
Compliant Chip Card Reading Device	An Acceptance Device (excluding an ATM) capable of reading, communicating, and processing full data Transactions[1] from a Compliant Chip Card. [1] Processed by Acquirers certified by Visa to process full data. ID# 0024473 Edition: Apr 2020 | Last Updated: Apr 2018
Confidential Consumer Cardholder Information	A Payment Credential or other personally identifiable information relating to a consumer Cardholder. ID# 0026359 Edition: Apr 2020 | Last Updated: Apr 2020

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Confidential Enhanced Merchant-Level Data – US Region	Merchant-related data provided through Visa to an Issuer in connection with a Visa Commercial Card. This data includes all Enhanced Merchant-Level Data except for Non-Confidential Enhanced Merchant-Level Data, and is subject to the disclosure restrictions specified in the Visa Rules. ID# 0024477 Edition: Apr 2020 | Last Updated: Oct 2015
Consumer Device Cardholder Verification Method (CDCVM)	An Issuer-approved, Visa-recognized method for capturing the Cardholder Verification Method on a Mobile Payment Device. ID# 0026877 Edition: Apr 2020 | Last Updated: Apr 2015
Consumer Visa Check Card – US Region	A Visa Check Card that accesses a consumer's deposit, investment, or other asset account, including a fiduciary account. ID# 0024481 Edition: Apr 2020 | Last Updated: Oct 2014
Contactless	A Visa-approved wireless interface used to exchange information between a Visa Card and an Acceptance Device. ID# 0029308 Edition: Apr 2020 | Last Updated: Oct 2015
Convenience Fee	A fee charged by a Merchant for a bona fide convenience to the Cardholder (for example: an alternative channel outside the Merchant's customary payment channel) that is not charged solely for the acceptance of the Card. ID# 0027486 Edition: Apr 2020 | Last Updated: Apr 2020
Counterfeit Card	One of the following: • A device or instrument that is printed, embossed, or encoded so as to purport to be a Card, but that is not a Card because an Issuer did not authorize its printing, embossing, or encoding • An instrument that is printed with the authority of the Issuer and that is subsequently embossed or encoded without the authority of the Issuer • A Card that an Issuer has issued and that is altered or re-fabricated, except one on which the only alteration or re-fabrication comprises modification of the signature panel or Cardholder signature ID# 0024495 Edition: Apr 2020 | Last Updated: Apr 2010
Country of Domicile	The country in which a Member has its principal place of business.

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0024499 Edition: Apr 2020 | Last Updated: Apr 2010
Credit Bureau – US Region	For purposes of Visa Advanced ID Solutions and Strategic Bankruptcy Solutions, a company that is required or has agreed to comply with the requirements applicable to consumer reporting agencies under the Federal Fair Credit Reporting Act. This includes a company that receives Member information pursuant to the ID Analytics, ID Score Plus, or Credit Optics components of Visa Advanced ID Solutions, or that provides card account numbers identified from bankruptcy petitions filed in US bankruptcy courts, to Strategic Bankruptcy Solutions.
	ID# 0024524 Edition: Apr 2020 | Last Updated: Oct 2014
Credit Card	In the AP Region, CEMEA Region, Europe Region, LAC Region, US Region: A Card linked to a secured or unsecured open-ended credit account, including revolving or non-revolving consumer, business, or commercial credit or charge accounts, or a credit account or equivalent as defined under applicable laws or regulations. An account is not a credit account if the credit results from the incidental extension of credit such as overdraft or minimum balance protection or similar services. In the Canada Region: A Card other than a Visa Debit Category Card.
	ID# 0027534 Edition: Apr 2020 | Last Updated: Apr 2020
Credit Optics – US Region	A feature of Visa Advanced ID Solutions that provides US Members with a score and related reason code(s) provided by ID Analytics, Inc. The information predicts the potential financial loss associated with approving an application for a new, or management of an existing, Card, non-Visa card, or other Visa or non-Visa product. The results are based on an assessment of the identity risk and application behavior of a consumer and the credit risk and application behavior of other similar consumers.
	ID# 0025783 Edition: Apr 2020 | Last Updated: Oct 2014
Credit Reporting Improvement Service – US Region	A service that supports an Issuer by monitoring the reporting and handling of credit bureau data.
	ID# 0024526 Edition: Apr 2020 | Last Updated: Oct 2014
Credit Transaction	A Transaction representing a Merchant's refund or price adjustment credited to a Cardholder's account.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0024527 Edition: Apr 2020 | Last Updated: Apr 2016
Credit Transaction Receipt	A Transaction Receipt evidencing a Merchant's refund or price adjustment to be credited to a Cardholder's account.
	ID# 0024528 Edition: Apr 2020 | Last Updated: Apr 2010
Cruise Line	A Merchant that sells tickets for, and provides, travel and overnight accommodations on a ship or boat.
	ID# 0024532 Edition: Apr 2020 | Last Updated: Apr 2016
Cryptogram	A value resulting from a combination of specific key data elements that are used to validate the source and integrity of data.
	ID# 0024533 Edition: Apr 2020 | Last Updated: Apr 2010
Currency Conversion Rate	A rate set by Visa from the range of rates available in wholesale currency markets for the applicable Processing Date, which rate may vary from the rate Visa itself receives; or the rate mandated by a government or a governing body in the country in which the Transaction occurred for the applicable Processing Date.
	The Visa rate may be adjusted by application of an Optional Issuer Fee as determined by the Issuer when VisaNet converts the Transaction Currency to the Billing Currency. However, when VisaNet converts the Transaction Currency to the Acquirer's Settlement Currency, or to the Issuer's Settlement Currency, the rate is applied by Visa and may not be adjusted.
	In the Europe Region: One of the following:
	• For Transactions outside of the Europe Region, the currency conversion rate set by Visa from the range of rates available in the wholesale currency markets for the applicable Processing Date, which rate may vary from the rate Visa itself receives
	• Either:
	– For Domestic or Intraregional Transactions where either Member is connected to BASE II, the currency conversion rate set by Visa from the range of rates available in the wholesale currency markets for the applicable Processing Date, which rate may vary from the rate Visa itself receives
	– For Domestic or Intraregional Transactions where the Member is connected to the Visa Europe Clearing and Settlement

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	Service, the currency conversion rate set by Visa from the range of rates available in the wholesale currency markets for the applicable Processing Date, which rate may vary from the rate Visa itself receives
	
	• Either:
	
	  – For Interregional Transactions where the Member is connected to BASE II, the currency conversion rate set by Visa from the range of rates available in the wholesale currency markets for the applicable Processing Date, which rate may vary from the rate Visa itself receives
	
	  – For Interregional Transactions where the Member is connected to the Visa Europe Clearing and Settlement Service, the currency conversion rate set by Visa from the range of rates available in the wholesale currency markets for the applicable Processing Date, which rate may vary from the rate Visa itself receives
	
	• A rate mandated by a government or a governing body in effect for the applicable Processing Date for a Transaction
	
	An Issuer shall set the conversion rate to its Cardholder and an Acquirer shall set the conversion rate to its Merchant, as specified in applicable laws and regulations.
	
	ID# 0024534 Edition: Apr 2020 | Last Updated: Oct 2016

Custom Payment Services (CPS)	A Visa payment service that accommodates specific payment environments with an identifier that remains with the Transaction throughout its life cycle. **ID# 0024536** Edition: Apr 2020 | Last Updated: Apr 2010
D	
Debit Card	A Card linked to a demand deposit account, checking account, current account, negotiable order of withdrawal account, or savings account held at a financial institution, or a debit account or equivalent as defined under applicable laws or regulations. **ID# 0025287** Edition: Apr 2020 | Last Updated: Apr 2020
Debit Card Cost of Acceptance – US Region and US Territories	In the US Region, US Territory: The amount of the cap for debit card transactions established by the Board of Governors of the Federal Reserve System pursuant to Federal Reserve Regulation II, 12 CFR Part 235, and which is subject to change.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0027530 Edition: Apr 2020 | Last Updated: Oct 2014
Debt	Money owed by one party (debtor) to another party (creditor). Debt includes, but is not limited to, any of the following: • The obligation to repay money in connection with: loans; credit card balances • Money advanced on goods previously purchased • Repayments that include interest (expressly or implicitly) The following are not treated as Debt for the purpose of the Visa Rules: • Lease payments, where ownership of the goods does not automatically pass to the lessee at the end of the lease • Interest-free Partial Payment • Late payment fees that are incentives to pay on time and are not related to the amount owed are not considered interest • Repayment of an overdue obligation that has not been charged-off and transferred from the original owner to a third party and does not include interest (expressly or implicitly) ID# 0030649 Edition: Apr 2020 | Last Updated: New
Decline Response	An Authorization Response where the Transaction was declined. ID# 0024548 Edition: Apr 2020 | Last Updated: Apr 2010
Deferred Clearing Transaction	A Transaction or process wherein Transactions are authorized, cleared, and settled in 2 separate messages. ID# 0024551 Edition: Apr 2020 | Last Updated: Oct 2016
Deferred Debit Card – Europe Region	A Card linked to an account whereby the Transactions are accumulated with other Transactions on a deferred basis, a statement is issued and the Cardholder is required to pay the outstanding balance in full. ID# 0029709 Edition: Apr 2020 | Last Updated: Oct 2016
Deferred Payment Transaction – US Region	A Transaction completed in a Card-Absent Environment for which the Cardholder is billed once, no more than 90 calendar days after the first shipment of merchandise. ID# 0024552 Edition: Apr 2020 | Last Updated: Oct 2017

Glossary

Visa Core Rules and Visa Product and Service Rules

Deferred Settlement	The Settlement funds transfer of a Transaction, according to the Member's instructions in the Clearing Record that occurs more than 2 business days after the Processing Date.
	ID# 0029032 · Edition: Apr 2020 | Last Updated: Oct 2014
Delegated Authentication Program – Europe Region	In the Europe Region: A Visa program that supports the delegation of strong customer authentication by an Issuer to a Strong Customer Authentication Delegate.
	ID# 0030621 · Edition: Apr 2020 | Last Updated: Apr 2019
Deposit	The submission of a Transaction by a Merchant, Marketplace, Payment Facilitator, or Staged Digital Wallet Operator to an Acquirer, resulting in a credit or debit to the Merchant's, Sponsored Merchant's, Marketplace's, Payment Facilitator's, or Staged Digital Wallet Operator's account.
	ID# 0024556 · Edition: Apr 2020 | Last Updated: Oct 2019
Deposit-Only Account Number	An Account Number established by an Issuer, used exclusively to receive an Original Credit Transaction on behalf of its Cardholder.
	ID# 0024554 · Edition: Apr 2020 | Last Updated: Oct 2016
Diamond Design	A Visa-Owned Mark, used as an element of the Plus Symbol, consisting of 3 triangles with an open space in the lower right-hand corner, arranged to form an outline of the symbol "+."
	ID# 0024558 · Edition: Apr 2020 | Last Updated: Apr 2010
Digital Certificate	A digitally signed credential used to authenticate the owner of the credential or to ensure the integrity and confidentiality of the message it is signing.
	ID# 0024559 · Edition: Apr 2020 | Last Updated: Apr 2010
Digital Wallet Operator (DWO)	A Third Party Agent that operates a Pass-Through Digital Wallet or Staged Digital Wallet.
	ID# 0029530 · Edition: Apr 2020 | Last Updated: Oct 2017
Direct (Immediate) Debit Card – Europe Region	A Card linked to a current (or deposit access) account to which a Transaction is debited immediately (in a maximum of two working days) on receipt of the Transaction by the Issuer.
	ID# 0029710 · Edition: Apr 2020 | Last Updated: Oct 2016

Glossary	
	Glossary

Visa Core Rules and Visa Product and Service Rules

Dispute	A Transaction that an Issuer returns to an Acquirer. ID# 0029463 — Edition: Apr 2020 | Last Updated: Apr 2018
Dispute Response	A Clearing Record that an Acquirer presents to an Issuer through Interchange after a Dispute. ID# 0029464 — Edition: Apr 2020 | Last Updated: Apr 2018
Domestic Transaction	A Transaction where the Issuer of the Card used is located in the Transaction Country. ID# 0024568 — Edition: Apr 2020 | Last Updated: Apr 2010
Domiciled Institution – LAC Region	A deposit-taking financial institution or a payment institution that is authorized by the Brazil Central Bank, and is used by a Merchant or a Sponsored Merchant for an Acquirer or a Payment Facilitator to deposit payments. ID# 0029506 — Edition: Apr 2020 | Last Updated: Apr 2017
Dual-Issuer Branded Visa Commercial Card	A Visa Commercial Card, issued by a Member participating in the Visa Multinational Program, that identifies the Lead Bank on the Card front and the Partner Bank on the Card back, as specified in the *Visa Multinational Program Guide*. ID# 0026028 — Edition: Apr 2020 | Last Updated: Oct 2014
Dynamic Card Verification Value (dCVV)	A Card Verification Value dynamically generated by a contact or Contactless Chip Card for inclusion in the Authorization message (for example: as part of the Magnetic-Stripe data). ID# 0025503 — Edition: Apr 2020 | Last Updated: Oct 2015
Dynamic Currency Conversion	Either: • The conversion of the purchase price of goods or services from the currency in which the price is displayed to another currency. That currency becomes the Transaction Currency. • An ATM Transaction in which the Transaction Currency is different to the currency disbursed. ID# 0024574 — Edition: Apr 2020 | Last Updated: Apr 2019
Dynamic Data Authentication	A cryptographic value generated by a Chip on a Card in an offline environment that uses Transaction-specific data elements and is verified by a Chip-Reading Device to protect against skimming.

Glossary	

Visa Core Rules and Visa Product and Service Rules

	ID# 0024575 Edition: Apr 2020 | Last Updated: Apr 2010
E	
Edit Package	The software that Visa supplies to VisaNet Processors to: • Validate Interchange data • Process Interchange data sent from the VisaNet Processor to Visa • Process incoming Transactions received from Visa **ID# 0024577** Edition: Apr 2020 | Last Updated: Apr 2010
Electronic Capability	Point-of-Transaction Capability where all of the following are true: • Authorization is required (or the terminal is capable of reading and acting upon the Service Code in the Magnetic Stripe or information provided in the Chip or, in the AP Region, QR code) • Authorization Response is obtained Online, or as instructed by the Issuer • Authorization Response and Transaction Receipt data are captured electronically **ID# 0024582** Edition: Apr 2020 | Last Updated: Apr 2020
Electronic Commerce Indicator	A value used in an Electronic Commerce Transaction to indicate the Transaction's level of authentication and security. **ID# 0026401** Edition: Apr 2020 | Last Updated: Oct 2014
Electronic Commerce Merchant	A Merchant that conducts the sale of goods or services electronically over the internet and other networks. **ID# 0024584** Edition: Apr 2020 | Last Updated: Oct 2014
Electronic Commerce Transaction	A Transaction between a Merchant and Cardholder over the internet or other networks using a terminal, personal computer, or other Cardholder device. **ID# 0024587** Edition: Apr 2020 | Last Updated: Oct 2016
Electronic Documentation Transfer Method – Europe Region	An electronic documentation transfer method approved by Visa for use by Europe Members. This method may be either: • A web-based application, such as Visa Resolve Online (VROL) • An approved, secure electronic method

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0029712 Edition: Apr 2020 | Last Updated: Oct 2016
Electronic Imprint	The reading and printing or capture of Card information at a Magnetic-Stripe Terminal or a Chip-Reading Device. In the AP Region: This also applies to a QR code Transaction with Full-Chip Data.
	ID# 0024593 Edition: Apr 2020 | Last Updated: Apr 2020
Emergency Card Replacement	A temporary Card that Visa Global Customer Assistance Services or the Issuer or its Agent provides to replace a Cardholder's damaged, lost, or stolen Card.
	ID# 0024610 Edition: Apr 2020 | Last Updated: Apr 2020
Emergency Cash Disbursement	A Cash Disbursement by a Member or its agent, including Visa Global Customer Assistance Services, to a Cardholder who needs emergency cash.
	ID# 0024605 Edition: Apr 2020 | Last Updated: Apr 2019
Emergency Service Location	A Visa Issuer-affiliated Branch pre-registered in the Visa Global Customer Assistance Services where a Cardholder may receive an Emergency Cash Disbursement or Emergency Card Replacement.
	ID# 0024612 Edition: Apr 2020 | Last Updated: Apr 2019
EMV Integrated Circuit Card Specifications for Payment Systems (EMV)	Technical specifications developed (jointly by Europay International, MasterCard International, and Visa International) to provide standards for processing debit and credit Transactions and ensure global interoperability for the use of Chip technology in the payment industry.
	ID# 0024620 Edition: Apr 2020 | Last Updated: Oct 2014
EMV PIN-Compliant	A Chip-Reading Device that complies with the PIN requirements of the Payment Card Industry Security Standards Council.
	ID# 0024622 Edition: Apr 2020 | Last Updated: Oct 2014
EMV-Compliant	A Card or terminal application that complies with the requirements specified in the *EMV Integrated Circuit Card Specifications for Payment Systems (EMV)*.
	ID# 0024617 Edition: Apr 2020 | Last Updated: Oct 2016
Enhanced Data	Data provided through Visa to an Issuer. Such data may include either or both:

	• Enhanced Merchant-Level Data (including data for a Sponsored Merchant or a Payment Facilitator) • Enhanced Transaction-Level Data ID# 0026463 Edition: Apr 2020 | Last Updated: Oct 2015
Enhanced Merchant-Level Data	Merchant- or Sponsored Merchant-related data (including Payment Facilitator data) provided through Visa to an Issuer. Such data includes: • Merchant street address • Merchant telephone number • Incorporation status • Owner's name ID# 0026464 Edition: Apr 2020 | Last Updated: Oct 2015
Enhanced Transaction-Level Data	Transaction-related data provided through Visa to an Issuer. Such data includes: • Accounting code • Sales tax or value-added tax • Description of items purchased, cost per unit, number of units • Vehicle fleet data (vehicle/driver ID, odometer reading) • Detailed itinerary information (Airline, origination/destination, class of travel) • For an Ancillary Purchase Transaction, all required data elements ID# 0024631 Edition: Apr 2020 | Last Updated: Oct 2015
Estimated Authorization Request	An Authorization Request for the amount that a Merchant expects a Cardholder to spend in an individual Transaction and that is submitted before the final Transaction amount is known. ID# 0029521 Edition: Apr 2020 | Last Updated: Oct 2017
EU Passporting – Europe Region	A system which allows payment service providers legally established in one member state of the European Economic Area to provide their services cross-border in the other member states of the European Economic Area either directly or through a physical establishment subject to meeting formal notification and approval requirements of the home and host regulator.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0029715 Edition: Apr 2020 | Last Updated: Oct 2016
European Economic Area – Europe Region	The member states of the European Union, and Iceland, Liechtenstein, and Norway.
	ID# 0029716 Edition: Apr 2020 | Last Updated: Oct 2016
European Economic Area Transaction – Europe Region	In the Europe Region: A Transaction initiated using a Card issued within the European Economic Area (EEA) and accepted at a Merchant Outlet located within the European Economic Area.
	ID# 0030653 Edition: Apr 2020 | Last Updated: Oct 2019
European Union	The following: Austria; Belgium; Bulgaria; Croatia; Cyprus; Czech Republic; Denmark; Estonia; Finland (including Aland Islands); France; Germany; Gibraltar;[1] Greece; Hungary; Republic of Ireland; Italy; Latvia; Lithuania; Luxembourg; Malta; Netherlands; Poland; Portugal (including Azores, Madeira); Romania; Slovakia; Slovenia; Spain (including Canary Islands, Ceuta, Melilla); Sweden; United Kingdom.[1] [1] **Effective through 31 January 2020**
	ID# 0030116 Edition: Apr 2020 | Last Updated: Apr 2020
Exception File	A VisaNet file of Account Numbers that a Member accesses Online, for which the Issuer has predetermined an Authorization Response. The Exception File supports: • Stand-In Processing • Positive Cardholder Authorization Service • Production of the Card Recovery Bulletin In the Europe Region: A file of Account Numbers for which the Issuer has predetermined an Authorization Response, which a Member accesses Online.
	ID# 0024634 Edition: Apr 2020 | Last Updated: Oct 2016
Expired Card	A Card on which the embossed, encoded, printed, or otherwise applicable expiration date has passed.
	ID# 0024638 Edition: Apr 2020 | Last Updated: Oct 2019
F	
Face-to-Face Environment	An environment in which a Transaction is completed under all of the following conditions:

	Glossary

Visa Core Rules and Visa Product and Service Rules

	• Card or Contactless Payment Device used to complete the Transaction is present • Cardholder is present • Individual representing the Merchant or Acquirer is available to complete the Transaction ID# 0024643 Edition: Apr 2020 | Last Updated: Oct 2014
Fallback Transaction	An EMV Chip Card Transaction initially attempted at a Chip-Reading Device, where the device's inability to read the Chip prevented the Transaction from being completed using the Chip data, and the Transaction is instead completed using an alternate means of data capture and transmission. ID# 0024645 Edition: Apr 2020 | Last Updated: Apr 2020
Fast Funds	A service that requires a participating Recipient Issuer to make funds available to a Cardholder within 30 minutes of receipt and approval of an incoming Original Credit Transaction initiated as an Online Financial Transaction. ID# 0026077 Edition: Apr 2020 | Last Updated: Oct 2018
Fee Collection Transaction	A transaction used to collect financial obligations of a Member arising out of the Visa Rules, the Visa Charter Documents, or other requirements adopted by Visa. ID# 0024647 Edition: Apr 2020 | Last Updated: Oct 2015

Fee Schedule	One of the following:
	
	• *Visa Asia-Pacific Fee Schedule*
	• *Visa Canada Fee Schedule*
	• *Visa CEMEA Fee Schedule*
	• *Visa Europe Fee Schedule:*
	   – *Visa Europe Fee Schedule – Non-EEA*
	   – *Visa Europe Fee Schedule – Non-Regulated*
	   – *Visa Europe Fee Schedule – Scheme*
	• *Visa LAC Fee Schedule*
	• *Visa U.S.A. Fee Schedule*
	• Any domestic or local Visa fee schedule

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	ID# 0027310 Edition: Apr 2020 | Last Updated: Oct 2016
Floor Limit	A currency amount that Visa has established for a Transaction, above which Online Authorization is required.
	ID# 0024654 Edition: Apr 2020 | Last Updated: Oct 2018
Fraud Activity	A Transaction that an Issuer reports as fraudulent when either a: • Fraudulent user used a Card or its Payment Credential • Card was obtained through misrepresentation of identification or financial status
	ID# 0024659 Edition: Apr 2020 | Last Updated: Apr 2020
Fulfillment	A document image that the Acquirer supplies in response to a Retrieval Request.
	ID# 0024661 Edition: Apr 2020 | Last Updated: Apr 2011
Full-Chip Data	Data that complies with all of the following: • Conforms to EMVCo minimum requirements • Supports cryptographic validation online • Records the Card and terminal interactions completed during a Transaction
	ID# 0024662 Edition: Apr 2020 | Last Updated: Oct 2016
Functional Type	Any mixture of alphanumeric characters or graphics that denotes participation in a program or benefit (for example: a loyalty or rewards program, an identification number, a bar code, or a QR code that can be scanned or read by an electronic reader or application enabling access to a membership or website/application).
	ID# 0029512 Edition: Apr 2020 | Last Updated: Apr 2017
Funds Disbursement	A transaction used by a Member or Visa to disburse funds to a Clearing Processor.
	ID# 0024665 Edition: Apr 2020 | Last Updated: Oct 2016
Funds Transfer Settlement Reporting Entity	An endpoint within a Visa Settlement hierarchy associated with one or more Settlement Reporting Entities.
	ID# 0026048 Edition: Apr 2020 | Last Updated: Apr 2012

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

G	
General Member – Canada Region	A customer of Visa Canada in the category of "General Customer" as defined in *Appendix E to the Canada Regional Operating Regulations*. ID# 0024671 — Edition: Apr 2020 | Last Updated: Oct 2014
Global Brand Protection Program	A global program that monitors Acquirers, Merchants, Marketplaces, Payment Facilitators, Sponsored Merchants, and Digital Wallet Operators to ensure that these entities do not: • Process illegal Transactions or are not associated with illegal activity • Engage in potentially deceptive marketing practices, as defined in the *Visa Global Brand Protection Program Guide for Acquirers* • Process Transactions that may adversely affect the goodwill of the Visa system ID# 0026388 — Edition: Apr 2020 | Last Updated: Apr 2018
Global Co-Branded Card	A Card that: • Is issued by one or more Issuers that has a contractual relationship with a Global Co-Branding Partner • Bears the Trade Name or Mark of the Global Co-Branding Partner on the front of the Card • May offer a Cardholder tangible benefits for Card usage and loyalty (for example: rebates, discounts, airline miles) ID# 0024675 — Edition: Apr 2020 | Last Updated: Oct 2014
Global Co-Branding Partner	A Member or non-Member that has a contractual relationship for the issuance of Global Co-Branded Cards in one or more Visa Regions and countries. ID# 0024676 — Edition: Apr 2020 | Last Updated: Oct 2018
Global Compromised Account Recovery	In the AP Region, Canada Region, CEMEA Region, LAC Region, and US Region: A Visa program by which Visa allocates to affected Issuers a portion of the operating expenses that are associated with an Account Data Compromise Event involving a compromise of either: • In a Card-Absent Environment, a Chip Card's Account Number and expiration date • In a Card-Present Environment, a Chip Card's Account Number and

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	Card Verification Value
	ID# 0026034 Edition: Apr 2020 | Last Updated: Apr 2018
Global Member Billing Solution	The primary billing system used by Visa.
	ID# 0024680 Edition: Apr 2020 | Last Updated: Oct 2011
Group Member	In the AP Region, Canada Region, CEMEA Region, LAC Region, and US Region: A Member as defined under the *Visa International Certificate of Incorporation and By-Laws* Section 2.21.
	ID# 0024685 Edition: Apr 2020 | Last Updated: Oct 2016
Guaranteed Reservation	A reservation made by a Cardholder who provides a Payment Credential, but no payment, at the time of reservation to ensure that accommodation, merchandise, or services will be available as reserved and agreed with the Merchant.
	ID# 0029265 Edition: Apr 2020 | Last Updated: Apr 2020
H	
Health Care Merchant – US Region	A Merchant, other than a pharmacy, whose primary business is providing health care services and that uses one of the following MCCs: 4119, 5975, 5976, 7277, 8011, 8021, 8031, 8041, 8042, 8043, 8044, 8049, 8050, 8062, 8071, 8099.
	ID# 0024698 Edition: Apr 2020 | Last Updated: Oct 2014
Health Reimbursement Arrangement (HRA) – US Region	An employer-funded Prepaid Card program that reimburses employees, in accordance with IRS regulations, for qualified out-of-pocket medical expenses not covered by the employer's health care plan.
	ID# 0024699 Edition: Apr 2020 | Last Updated: Apr 2020
Health Savings Account (HSA) – US Region	A Prepaid Card program operated in accordance with IRS regulations that enables participants of a qualified high-deductible health plan to access funds contributed by an employee and/or employer for qualified out-of-pocket health care expenses.
	ID# 0024700 Edition: Apr 2020 | Last Updated: Apr 2020
Healthcare Auto-Substantiation – US Region	A process that enables an Issuer to automatically substantiate the dollar amount of qualifying medical purchases in the Authorization Request for a Visa Flexible Spending Account (FSA) or a Visa Health Reimbursement Arrangement (HRA) Transaction. Issuers of these Cards,

Glossary	

Glossary

Visa Core Rules and Visa Product and Service Rules

	and any Agents that process Transactions for such Cards, must perform Healthcare Auto-Substantiation.
	ID# 0024696 Edition: Apr 2020 | Last Updated: Oct 2016
High-Brand Risk Merchant	A Merchant classified by Visa as high-brand risk, as specified in *Section 10.4.6.1, High-Brand Risk Merchants*.
	ID# 0026389 Edition: Apr 2020 | Last Updated: Apr 2020
High-Brand Risk Sponsored Merchant	A Sponsored Merchant classified by Visa as high-brand risk, as specified in *Section 10.4.6.1, High-Brand Risk Merchants*, that contracts with a Payment Facilitator to obtain payment services.
	ID# 0026390 Edition: Apr 2020 | Last Updated: Apr 2020
High-Brand Risk Transaction	A Transaction performed by a High-Brand Risk Merchant, High-Risk Internet Payment Facilitator, High-Brand Risk Sponsored Merchant, or Digital Wallet Operator classified by Visa as high-brand risk, as specified in *Section 10.4.6.1, High-Brand Risk Merchants*.
	ID# 0026391 Edition: Apr 2020 | Last Updated: Apr 2020
High-Risk Internet Payment Facilitator	A Payment Facilitator that: • Enters into a contract with an Acquirer to provide payment services to High-Risk Merchants, High-Brand Risk Merchants, High-Risk Sponsored Merchants, or High-Brand Risk Sponsored Merchants • Includes one or more Sponsored Merchants classified by Visa as high-brand risk, as specified in *Section 10.4.6.1, High-Brand Risk Merchants*
	ID# 0026392 Edition: Apr 2020 | Last Updated: Apr 2020
Home Country – Europe Region	The country in which a Member has its principal place of business and is authorized under applicable national law to provide payment services.
	ID# 0029719 Edition: Apr 2020 | Last Updated: Oct 2016
Host Country – Europe Region	A country, other than a Home Country, in which a Member has satisfied the requirements of the competent domestic authority to provide payment services.
	ID# 0029720 Edition: Apr 2020 | Last Updated: Oct 2016

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

I	
ID Score Plus – US Region	A feature of Visa Advanced ID Solutions that provides Members with a score and related reason code(s) provided by ID Analytics, Inc. The score assesses the risk associated with an identity in connection with an application for a Card or non-Visa card or other Visa or non-Visa product.
	ID# 0024711 Edition: Apr 2020 | Last Updated: Oct 2014
Imprint	Cardholder data transferred from a Card to a Transaction Receipt to complete a Transaction. There are 2 kinds of imprints: • Electronic Imprint • Manual Imprint
	ID# 0024713 Edition: Apr 2020 | Last Updated: Apr 2010
In-Transit Transaction	A Transaction reflecting the purchase of merchandise, services, or gambling on board a ship, boat, bus, aircraft, ferry, or train.
	ID# 0024717 Edition: Apr 2020 | Last Updated: Apr 2016
Incremental Authorization Request	An Authorization Request that both: • Follows an approved Estimated Authorization Request or Initial Authorization Request • Is for an additional amount that a Merchant expects a Cardholder to spend or that the Cardholder has incurred in an individual Transaction
	ID# 0029522 Edition: Apr 2020 | Last Updated: Oct 2017
Indemnification	The act of indemnifying, defending, and holding harmless (see Indemnify).
	ID# 0030548 Edition: Apr 2020 | Last Updated: Apr 2018
Indemnify	To indemnify, defend, and hold harmless (see Indemnification).
	ID# 0030549 Edition: Apr 2020 | Last Updated: Apr 2018
Independent Sales Organization – Europe Region	An entity that is not eligible for Membership, has no direct connection to Visa, and provides a Member with bank card-related support services, such as: • Merchant solicitation

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	• Point-of-Transaction Acceptance Device installation and service • Transaction Receipt data capture and transmission • Cardholder solicitation ID# 0029721 Edition: Apr 2020 | Last Updated: Oct 2016
Initial Authorization Request	An Authorization Request for a capped amount or an amount based on an interim purchase or order and that is submitted before the final Transaction amount is known. ID# 0029523 Edition: Apr 2020 | Last Updated: Oct 2017
Installment Transaction	**Effective through 24 January 2020** A Transaction in a series of Transactions that use a Stored Credential and that represent Cardholder agreement for the Merchant to initiate one or more future Transactions over a period of time for a single purchase of goods or services. **Effective 25 January 2020** A Transaction in a series of Transactions that represents Cardholder agreement for the Merchant to initiate one or more future Transactions over a fixed period of time (not to exceed one year between Transactions) for a single purchase of goods or services, or the repayment of a single Debt. ID# 0024724 Edition: Apr 2020 | Last Updated: Apr 2020
Instant Card Personalization	The ability to instantly personalize Cards at a location other than a Member's card manufacturing facility to allow any of the following: • Immediate delivery of the Card at the Branch • Respond immediately to a request for an emergency replacement of a Cardholder's lost or stolen Card ID# 0025525 Edition: Apr 2020 | Last Updated: Apr 2020
Instant Card Personalization Issuance Agent	A Third Party Agent that performs instant Card personalization and issuance for an Issuer. ID# 0025526 Edition: Apr 2020 | Last Updated: Oct 2014
Integrated Card Verification Value (iCVV)	An alternate Card Verification Value that an Issuer must encode in the Magnetic-Stripe Image on a Chip instead of the Card Verification Value contained in the Magnetic Stripe of the Chip Card. ID# 0024710 Edition: Apr 2020 | Last Updated: Oct 2017
Interchange	The exchange of Clearing Records between Members. The Visa Rules

	refer to the following types of Interchange: • Domestic Interchange • International Interchange ID# 0024729 Edition: Apr 2020 | Last Updated: Oct 2014
Interchange File	An electronic file containing a Member's Interchange data. ID# 0024732 Edition: Apr 2020 | Last Updated: Apr 2010
Interchange Reimbursement Fee (IRF)	A fee between Acquirers and Issuers in the Clearing and Settlement of an Interchange Transaction. ID# 0024733 Edition: Apr 2020 | Last Updated: Oct 2017
Interlink Program	A program through which an Interlink participant (acting as an Interlink issuer) provides Point-of-Transaction services to Interlink cardholders, Interlink merchants, or both, as specified in the *Interlink Network, Inc. Bylaws, Interlink Core Rules and Interlink Product and Service Rules,* and the Visa Rules. ID# 0024737 Edition: Apr 2020 | Last Updated: Oct 2014
Interlink Program Marks	The combination of the Interlink Wordmark, the Network Design Mark, or any other service Marks that Visa adopts for use with the Interlink Program. ID# 0024738 Edition: Apr 2020 | Last Updated: Oct 2015
Intermediary Bank	A depository institution, specified by a Member or by Visa, through which a Settlement funds transfer must be processed for credit to a Settlement account at another depository institution. ID# 0024741 Edition: Apr 2020 | Last Updated: Apr 2010
International Airline	Either: • An Airline that sells tickets directly in its own name in 2 or more countries, operates scheduled flights between 2 or more countries, or both • Its authorized agent that sells airline tickets on behalf of the Airline (except in the Europe Region) ID# 0024742 Edition: Apr 2020 | Last Updated: Oct 2016
International Settlement	A Settlement Service used to settle all Transactions that do not

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Service	participate in a National Net Settlement Service, an Area Net Settlement Service, or other Settlement Services. ID# 0029723 — Edition: Apr 2020 | Last Updated: Oct 2016
International Transaction	A Transaction where the Issuer of the Card used is not located in the Transaction Country. In the US Region, US Territory: This does not apply for US Covered Visa Debit Card Transactions in the US Region or a US Territory for routing and Interchange Reimbursement Fee (IRF) purposes. ID# 0024752 — Edition: Apr 2020 | Last Updated: Oct 2017
Interregional Transaction	A Transaction where the Issuer of the Card is not located in the Visa Region where the Transaction takes place. ID# 0024762 — Edition: Apr 2020 | Last Updated: Oct 2017
Intraregional Transaction	A Transaction where the Issuer of the Card is located in a country other than the Transaction Country, but in the same Visa Region. ID# 0024763 — Edition: Apr 2020 | Last Updated: Oct 2017
IRF Compliance	A process by which Visa resolves disputes between Members for a Member's violation of the Visa Rules or any applicable Interchange Reimbursement Fee (IRF) guide that causes an incorrect Interchange Reimbursement Fee rate to be applied to a large number of Transactions, resulting in a financial loss to another Member. ID# 0024735 — Edition: Apr 2020 | Last Updated: Oct 2017
Issuer	In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A Member that enters into a contractual relationship with a Cardholder for the issuance of one or more Card products. In the Europe Region: A Member that issues a Card to a Cardholder and maintains the contractual privity relating to the Card with that Cardholder. ID# 0024768 — Edition: Apr 2020 | Last Updated: Oct 2016
Issuers' Clearinghouse Service – US Region	A service developed jointly by Visa and MasterCard Worldwide that is designed to reduce Member losses from excessive credit applications and unauthorized use. ID# 0024769 — Edition: Apr 2020 | Last Updated: Oct 2014

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

J	
No glossary terms available for J.	
	ID# 0025512 Edition: Apr 2020 | Last Updated: Apr 2010

K	
Known Fare Transaction	A Contactless Transaction at an Unattended Cardholder-Activated Terminal at the turnstile, fare gate, or point of boarding of a Mass Transit Merchant where the Transaction amount is known before travel.
	ID# 0030047 Edition: Apr 2020 | Last Updated: Apr 2018

L	
LAC	Latin America and Caribbean.
	ID# 0024774 Edition: Apr 2020 | Last Updated: Apr 2010
Lead Bank	A Visa Multinational Program participant that initiates Multi-Country Issuing on behalf of a Multinational Company client.
	ID# 0026026 Edition: Apr 2020 | Last Updated: Apr 2012
Level II Enhanced Data – US Region	Data provided to Visa in connection with a Commercial Visa Product Transaction that includes the sales tax amount, customer code (cost center, general ledger number, order/invoice number), and additional data for T&E Transactions.
	ID# 0024778 Edition: Apr 2020 | Last Updated: Oct 2017
Liability	Any and all damages (including lost profits or savings, indirect, consequential, special, exemplary, punitive, or incidental), penalties, fines, expenses and costs (including reasonable fees and expenses of legal and other advisers, court costs and other dispute resolution costs), or other losses.
	ID# 0024779 Edition: Apr 2020 | Last Updated: Apr 2018
Licensee	An entity licensed to participate in the Visa or Visa Electron Program that is neither a: • Member • Member or owner of a Group Member
	ID# 0024780 Edition: Apr 2020 | Last Updated: Apr 2010
Limited Acceptance – Europe Region and US Region	In the Europe Region: A term describing the option to accept one or more, but not all, Product Categories by a Merchant located within the European Economic Area.

	Glossary	
	Glossary	
	Visa Core Rules and Visa Product and Service Rules	

	In the US Region: A term describing a Merchant's option to accept one category of Visa Cards and not another. Categories consist of both: • Visa Credit and Business Category • Visa Debit Category This definition does not apply to Visa Business Check Cards accepted as specified in _Section 5.9.12.1, Repayment of Debt_.	
	ID# 0024784	Edition: Apr 2020 | Last Updated: Oct 2017
Limited Acceptance Merchant – Europe Region and US Region	In the Europe Region: A Merchant located within the European Economic Area that chooses to accept one or more, but not all, Product Categories. In the US Region: A category of Merchant that accepts either, but not both: • Visa Credit and Business Category Cards • Visa Debit Category Cards	
	ID# 0024785	Edition: Apr 2020 | Last Updated: Apr 2017
Load Device – Europe Region	An ATM or stand-alone device that a Cardholder uses to add or remove value from a stored value application on a Chip Card.	
	ID# 0029724	Edition: Apr 2020 | Last Updated: Oct 2016
Load Transaction	A means of adding monetary value to a Card (in the Europe Region, only at a Point-of-Transaction Acceptance Device).	
	ID# 0024791	Edition: Apr 2020 | Last Updated: Oct 2016
Lodging Merchant	A Merchant that sells overnight accommodations at a fixed location that are purchased for a limited period of time. For the purposes of the Visa Rules, Lodging Merchants are hotels, motels, inns, bed and breakfast establishments, resorts, cabins, cottages, hostels, and apartments, condominiums, and houses rented as a short-term accommodation.	
	ID# 0024794	Edition: Apr 2020 | Last Updated: Oct 2017
Lost/Stolen Card Reporting	A service that adds an Account Number to the Exception File.	
	ID# 0024798	Edition: Apr 2020 | Last Updated: Apr 2019
M		

Glossary

Visa Core Rules and Visa Product and Service Rules

Magnetic Stripe	A magnetic stripe on a Card that contains the necessary information to complete a Transaction. ID# 0024808 Edition: Apr 2020 | Last Updated: Apr 2010
Magnetic-Stripe Data	Data contained in a Magnetic Stripe and replicated in a Chip. ID# 0024802 Edition: Apr 2020 | Last Updated: Apr 2010
Magnetic-Stripe Image	The minimum Chip payment data replicating the Magnetic Stripe information required to process an EMV-Compliant Transaction. ID# 0024803 Edition: Apr 2020 | Last Updated: Apr 2010
Magnetic-Stripe Terminal	A terminal that reads the Magnetic Stripe on a Card. ID# 0024806 Edition: Apr 2020 | Last Updated: Apr 2010
Mail/Phone Order	Purchase in a Card-Absent Environment where a Cardholder orders goods or services from a Merchant by telephone, mail, or other means of telecommunication. ID# 0029309 Edition: Apr 2020 | Last Updated: Oct 2015
Manual Cash Disbursement	A Cash Disbursement obtained with a Card in a Face-to-Face Environment. ID# 0024814 Edition: Apr 2020 | Last Updated: Apr 2020
Manual Imprint	An imprint of the embossed data on the front of the Card using a specifically-designed mechanical imprinting device. An impression taken from the Card using pencil, crayon, or other writing instrument does not qualify. ID# 0024815 Edition: Apr 2020 | Last Updated: Oct 2015
Mark	A word, name, design, symbol, distinctive sign, animation, sound, haptic, other designation, or any combination thereof, that Visa or any entity adopts to identify its goods or services. ID# 0024818 Edition: Apr 2020 | Last Updated: Apr 2020
Marketplace	An entity that brings together Cardholders and retailers on an electronic commerce website or mobile application and processes Transactions and receives Settlement on behalf of those retailers. ID# 0030075 Edition: Apr 2020 | Last Updated: Oct 2019

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Mass Transit Merchant	A Merchant that is assigned MCC 4111, 4112, or 4131 and completes a Mass Transit Transaction, Known Fare Transaction, or another method of fare collection using a Visa Card.
	ID# 0030054 — Edition: Apr 2020 | Last Updated: Apr 2018
Mass Transit Transaction	A Contactless Transaction at an Unattended Cardholder-Activated Terminal at the turnstile, fare gate, or point of boarding of a Mass Transit Merchant that uses the data derived from one or more taps of a Contactless Payment Device during a Travel Period to calculate the Transaction amount.
	ID# 0030053 — Edition: Apr 2020 | Last Updated: Apr 2018
Maximum Surcharge Cap – US Region and US Territories	In the US Region or a US Territory, the maximum US Credit Card Surcharge that a Merchant may assess on a Visa Credit Card Transaction, as may be revised from time to time and that is communicated via the Visa public website, *www.visa.com*.
	ID# 0027531 — Edition: Apr 2020 | Last Updated: Oct 2014
Member	A client of Visa U.S.A., Visa International, Visa Worldwide, Visa Europe Limited, or Visa International Servicios de Pago España, S.R.L.U. or a customer that has entered into a Services Agreement with Visa Canada. Requirements for membership are defined in the applicable Visa Charter Documents.
	The Services Agreement is a license or contract between Visa Canada and an entity that has a contract or license that allows the entity to participate in the Visa program or use the Visa-Owned Marks, including in accordance with the Visa Rules.
	ID# 0024822 — Edition: Apr 2020 | Last Updated: Oct 2016
Merchant	In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: An entity that accepts a Card for the sale of goods/services or to originate funds transfers to another Visa or non-Visa account, and submits the resulting Transaction to an Acquirer for Interchange, directly or via a Payment Facilitator. A Merchant may be a single Merchant Outlet or represent multiple Merchant Outlets.
	In the Europe Region: An entity that enters into an agreement with an Acquirer for the acceptance of Cards for purposes of originating either payment Transactions or funds transfer Transactions under the Visa-Owned Marks.

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0024828 Edition: Apr 2020 | Last Updated: Apr 2020
Merchant Agreement	A direct contract between a Merchant and an Acquirer or between a Sponsored Merchant and a Payment Facilitator containing their respective rights, duties, and obligations for participation in the Acquirer's Visa or Visa Electron Program.
	ID# 0024830 Edition: Apr 2020 | Last Updated: Apr 2015
Merchant Category Code (MCC)	A code designating the principal trade, profession, or line of business in which a Merchant is engaged.
	ID# 0024834 Edition: Apr 2020 | Last Updated: Oct 2016
Merchant Discount Rate – US Region and US Territories	In the US Region, US Territory: The fee, expressed as a percentage of the total Transaction amount that a Merchant pays to its Acquirer or VisaNet Processor for transacting on a credit card brand. The Merchant Discount Rate includes both: • The interchange rate, network set fees associated with the processing of a Transaction, network set fees associated with the acceptance of the network's brand, and the Acquirer set processing fees associated with the processing of a Transaction, irrespective of whether such fees and costs are paid via the Merchant discount or by check, withholding, offset, or otherwise; and • Any other services for which the Acquirer is paid via the mechanism of the per transaction merchant discount fee. Other than the fees listed in the first bullet above, the Merchant Discount Rate excludes any fees (such as the cost of rental of point-of-sale terminal equipment, for example) that are invoiced separately or not paid via the mechanism of the per transaction merchant discount fee.
	ID# 0027532 Edition: Apr 2020 | Last Updated: Oct 2014
Merchant Outlet	The Merchant location at which a Transaction is completed, for example: • Retail store • Stand-alone UCAT that is not located within a Merchant's premises • Electronic Commerce Merchant's website • Transit vehicle, such as a bus or ferry

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

	• Airplane
	ID# 0024842 Edition: Apr 2020 | Last Updated: Apr 2019
Merchant Service Charge – Europe Region	A fee that is set, and charged, by an Acquirer to a Merchant under a Merchant Agreement.
	ID# 0029726 Edition: Apr 2020 | Last Updated: Oct 2016
Merchant Verification Value (MVV)	An assigned value transmitted in the Transaction message used by Visa to identify an Acquirer or Merchant that is registered with Visa: • To assess specific fees • For other special Interchange treatment • For participation in select acceptance programs • For unique processing criteria The MVV consists of 10 digits, the first 6 of which are assigned by Visa. **Effective through 17 October 2020** This does not apply in the Europe Region.
	ID# 0026121 Edition: Apr 2020 | Last Updated: Apr 2020
Merger	A term used to describe any of the following: • Purchase of a Member organization by another organization where the acquired Member's charter is dissolved • Merging of two or more organizations into a single entity requiring a new charter
	ID# 0025531 Edition: Apr 2020 | Last Updated: Oct 2011
MIF – Europe Region	Multilaterally agreed interchange fee(s) paid by an Acquirer to a separate Issuer or vice versa.
	ID# 0029727 Edition: Apr 2020 | Last Updated: Oct 2016
MIF Plus Plus – Europe Region	Pricing in a Merchant Agreement where the Merchant Service Charge for Transactions referred to in the Merchant Agreement and on invoices is broken down into separate components comprising the MIF, all other fees applicable to Transactions, and the Acquirer's fee (including the margin).
	ID# 0029728 Edition: Apr 2020 | Last Updated: Oct 2016

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Minimum Spending Limit	The ability of a Cardholder to accumulate charges up to a predefined value during each or any statement cycle. For products with debit capabilities, Minimum Spending Limit is subject to available funds in the account of the Cardholder. ID# 0025673 Edition: Apr 2020 | Last Updated: Oct 2015
Mobile Acceptance Device – Europe Region	A Point-of-Transaction Acceptance Device that consists of a hardware accessory and any mobile device (including, but not limited to, mobile phones and tablets) owned or operated by a Merchant. ID# 0029729 Edition: Apr 2020 | Last Updated: Oct 2016
Mobile Money Agent – AP Region, CEMEA Region, and LAC Region	An entity that delivers Transaction services to Visa Mobile Prepaid account holders, including, but not limited to, customer registration, Card distribution, cash-ins, and cash-outs. ID# 0027166 Edition: Apr 2020 | Last Updated: Oct 2014
Mobile Money Consumer Authentication – AP Region, CEMEA Region, and LAC Region	A 2-part authentication process conducted by a Mobile Money Operator to verify a Visa Mobile Prepaid account holder. ID# 0027678 Edition: Apr 2020 | Last Updated: Oct 2014
Mobile Money Operator – AP Region, CEMEA Region, and LAC Region	A category of financial service providers that may include Members or non-deposit-taking financial institutions, such as mobile network operators and micro-finance institutions, that may use a Mobile Money Agent or branch network as its acquisition and service channel for Visa Mobile Prepaid account holders. ID# 0027167 Edition: Apr 2020 | Last Updated: Oct 2014
Mobile Payment Acceptance Solution	A payment acceptance application that uses a portable electronic device. The portable electronic device must exhibit both of the following characteristics: • Not solely dedicated to point-of-sale functions • The ability to wirelessly communicate across open networks The solution may also include a hardware attachment for the purpose of card reading and/or PIN entry. ID# 0027382 Edition: Apr 2020 | Last Updated: Oct 2014
Mobile Payment Device	A Contactless Payment Device that resides in a portable electronic device that can access a wireless network.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0026785 Edition: Apr 2020 | Last Updated: Oct 2014
Mobile Push Payment Transaction	An Original Credit Transaction initiated by a Visa account holder using a mobile device (for example: mobile phone, tablet) for the payment of goods or services, Cash-In, or Cash-Out. In the AP Region (Australia, New Zealand), Canada Region, Europe Region (except Romania), US Region: This is not available.
	ID# 0030586 Edition: Apr 2020 | Last Updated: Apr 2019
Money Transfer Original Credit Transaction	A funds transfer Transaction initiated by a Member that results in a credit to a Payment Credential for a purpose other than refunding a Visa purchase (for example: overseas remittances, gift transfers, Card payments).
	ID# 0026081 Edition: Apr 2020 | Last Updated: Apr 2020
Multi-Country Issuing	Within the Visa Multinational Program, a scenario in which a Lead Bank forms a relationship with a Partner Bank located in another country for the purpose of issuing Visa Commercial Card products to its Multinational Company clients. Multi-Country Issuing is identified in the *Visa Multinational Program Guide* as "Indirect Cross-Border Issuing."
	ID# 0026027 Edition: Apr 2020 | Last Updated: Oct 2014
Multinational Company	A commercial organization with operations, subsidiaries, and employees situated in more than one country (excluding franchise representatives, independently owned dealers, and joint ventures in which a Multinational Company participates), as specified in the *Visa Multinational Program Guide*.
	ID# 0024854 Edition: Apr 2020 | Last Updated: Oct 2014
N	
National Card Recovery File	A weekly file of all Account Numbers listed on an Exception File with a Pickup Response.
	ID# 0024857 Edition: Apr 2020 | Last Updated: Oct 2016
National Organization	In the AP Region, Canada Region, CEMEA Region, LAC Region, and US Region: An organization as defined under the *Visa International Certificate of Incorporation and By-Laws,* Section 16.01. In the Europe Region: An organization to which Visa delegates, in

Visa Core Rules and Visa Product and Service Rules

	whole or in part, its responsibility for the development, operation, and administration of Card programs and/or Card products in any country or countries in the Europe Region, including the following: • The development and implementation of products, services, systems, programs, and strategies to address unique market conditions within such country or countries • Coordination of Member activities (as relevant) • The promulgation of rules, regulations, and policies applicable to Members operating within such country or countries ID# 0024863 Edition: Apr 2020 | Last Updated: Apr 2020
New Channel	An environment in which payment is initiated via a terminal, personal computer or other device that does not use a standard Hypertext Markup Language (HTML) browser to process an Authentication Request. ID# 0024868 Edition: Apr 2020 | Last Updated: Oct 2015
No-Show Transaction	A Transaction resulting from a Cardholder's failure to cancel or claim a Guaranteed Reservation. ID# 0024869 Edition: Apr 2020 | Last Updated: Apr 2016
Non-Authenticated Security Transaction	An Electronic Commerce Transaction that uses data encryption for security but is not authenticated using an Authentication Method. ID# 0024871 Edition: Apr 2020 | Last Updated: Apr 2010
Non-Confidential Enhanced Merchant-Level Data – US Region	Merchant-related data provided through Visa to an Issuer in connection with a Visa Commercial Card, comprising only the following data elements: • Merchant name • Merchant street address • Merchant city, state, and ZIP code • Merchant telephone number ID# 0024872 Edition: Apr 2020 | Last Updated: Oct 2015
Non-Member Administrator – US Region	A VisaNet Processor permitted to sponsor Associate-type Members as specified in the *Visa U.S.A. Inc. Certificate of Incorporation and By-Laws*.

Glossary

	ID# 0029313 Edition: Apr 2020 | Last Updated: Oct 2016
Non-Reloadable Prepaid Card	A Prepaid Card that is funded with monetary value only once.
	ID# 0024880 Edition: Apr 2020 | Last Updated: Apr 2020
Non-Secure Transaction	An Electronic Commerce Transaction that has no data protection.
	ID# 0024881 Edition: Apr 2020 | Last Updated: Apr 2010
Non-Standard Card	A Card that does not comply with the plastic specifications in the *Visa Product Brand Standards*, requires Visa approval, and must both: • Provide the designated level of utility promised to the Cardholder • Contain the physical elements and data components required to complete a Transaction
	ID# 0024883 Edition: Apr 2020 | Last Updated: Apr 2020
Non-Visa Debit Transaction – US Region	An act between a Visa Check Card or Debit Card Cardholder and a merchant that results in the generation of a transaction on a debit network other than Visa.
	ID# 0024885 Edition: Apr 2020 | Last Updated: Apr 2020
Non-Visa-Owned Marks	The Marks used in conjunction with a program sponsored by Visa, but owned by a third party.
	ID# 0024884 Edition: Apr 2020 | Last Updated: Apr 2010
Nonfulfillment Message	A response to a Retrieval Request indicating that the Acquirer will not provide a copy.
	ID# 0024886 Edition: Apr 2020 | Last Updated: Oct 2016
Notification	Written notice delivered by mail, courier, facsimile, hand, email, or other electronic delivery method. Notification is effective when posted, sent, or transmitted by Visa to the Member or its Agent.
	ID# 0024887 Edition: Apr 2020 | Last Updated: Oct 2014
Numeric ID	Any identifier, other than a BIN or an Acquiring Identifier, assigned by Visa to a Member, VisaNet Processor, or Third Party Agent, including, but not limited to, processor control records (PCR), station IDs, issuing identifiers, alternate routing identifiers, Visa Resolve Online (VROL) identifiers, and encryption rule identifiers used to facilitate transaction processing.

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	ID# 0026475 Edition: Apr 2020 | Last Updated: Oct 2019
O	
Offline Authorization	An Issuer-controlled process that allows a Chip-initiated Authorization Request to be processed in a below-Floor Limit environment without sending the request to the Issuer.
	ID# 0024898 Edition: Apr 2020 | Last Updated: Oct 2018
Offline PIN Verification	A process used to verify the Cardholder's identity by comparing the PIN entered at the Chip-Reading Device to the PIN value contained in the Chip.
	ID# 0024902 Edition: Apr 2020 | Last Updated: Apr 2010
On-Us Transaction	A Transaction where an individual Member, represented by one Visa Business ID (BID), both: • Holds an issuing license and has issued the Card used in the Transaction • Holds an acquiring license and acquired the corresponding Merchant volume
	ID# 0024907 Edition: Apr 2020 | Last Updated: Apr 2020
Online	A method of requesting an Authorization through a communications network other than voice.
	ID# 0024910 Edition: Apr 2020 | Last Updated: Oct 2018
Online Card Authentication Cryptogram	A cryptogram generated by a Chip Card during a Transaction and used to validate the authenticity of the Card.
	ID# 0024912 Edition: Apr 2020 | Last Updated: Apr 2011
Online Financial Transaction	A Transaction that is authorized, cleared, and settled in a single online message.
	ID# 0024915 Edition: Apr 2020 | Last Updated: Apr 2010
Online Gambling	Any form of gambling provided over the internet or other networks by an Electronic Commerce Merchant, including, but not limited to, the following: • Betting • Lotteries

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	• Casino-style games • Funding an account established by the Merchant on behalf of the Cardholder for the purpose of gambling • Purchase of value for proprietary payment mechanisms, such as electronic gaming chips ID# 0029310 Edition: Apr 2020 | Last Updated: Apr 2018
Operating Certificate	In the AP Region, Canada Region, CEMEA Region, LAC Region, US Region: A report that a Member or Non-Member Administrator sends to Visa at a set pre-determined time, detailing its Card and Merchant statistics. In the Europe Region: The certificate supplied by each Member to Visa pursuant to Part B of the *Visa Europe Limited Membership Regulations*. ID# 0027826 Edition: Apr 2020 | Last Updated: Apr 2020
Operating Expense Recovery	The recovery amount provided to Issuers through the Global Compromised Account Recovery (GCAR) program associated with an Account Data Compromise Event. ID# 0026064 Edition: Apr 2020 | Last Updated: Apr 2018
Optional Issuer Fee	A fee that an Issuer may charge a Cardholder by the application of a percentage increase to the Currency Conversion Rate, which the Visa Systems use to determine the Transaction Amount in the Billing Currency for each International Transaction. ID# 0029314 Edition: Apr 2020 | Last Updated: Apr 2016
Order Form	A document bearing the Cardholder's signature, either written or electronic, authorizing goods or services to be charged to his/her account. An Order Form may be any of the following: • Mail order form • Recurring Transaction form • Preauthorized Healthcare Transaction form • Email or other electronic record that meets the requirements of applicable laws or regulations ID# 0024923 Edition: Apr 2020 | Last Updated: Apr 2018
Original Adjustment – US Region	A PIN-Authenticated Visa Debit Transaction completed and submitted through Interchange without an Authorization because the connection

Glossary	

	between the Merchant and its VisaNet Processor was inoperable
	ID# 0024924 Edition: Apr 2020 | Last Updated: Apr 2016
Original Credit Transaction	A Transaction initiated directly by an Acquirer, a Merchant, or an agent, or by an Acquirer on behalf of its Merchant or agent, that results in a credit to a Payment Credential for a purpose other than refunding a purchase.
	ID# 0024925 Edition: Apr 2020 | Last Updated: Apr 2020
Originating Acquirer	An Acquirer that initiates an Original Credit Transaction.
	ID# 0024926 Edition: Apr 2020 | Last Updated: Oct 2018
P	
Partial Authorization	An Authorization for an amount less than the amount requested by a Merchant for a Transaction.
	ID# 0024929 Edition: Apr 2020 | Last Updated: Oct 2016
Partial Payment	**Effective 25 January 2020** A Transaction in a series of Installment Transactions for the purchase of goods and services with both of the following characteristics: • There is no charge to the Cardholder, by the Merchant, for interest or imputed interest. • The agreement between the Cardholder and Merchant is completed before or at the time of first Transaction.
	ID# 0030638 Edition: Apr 2020 | Last Updated: New
Participant-Type Member	A Member of Visa characterized as a Participant, as defined in the applicable Visa Charter Documents.
	ID# 0024930 Edition: Apr 2020 | Last Updated: Apr 2019
Partner Bank	A Visa Multinational Program participant that partners with the Lead Bank in a Multi-Country Issuing scenario. The Partner Bank resides in a country that is different from the Lead Bank and issues Visa Commercial Card products on behalf of the Lead Bank.
	ID# 0026029 Edition: Apr 2020 | Last Updated: Oct 2014
Pass-Through Digital Wallet	Functionality provided by a Digital Wallet Operator (DWO) that does all of the following: • Can be used at more than one Merchant

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

	• Stores and transmits a Payment Credential • Is used by the DWO to complete a Transaction by transferring the Payment Credential to the Merchant without interrupting the flow of funds ID# 0029533 Edition: Apr 2020 | Last Updated: Apr 2020
Payment Account Reference (PAR)	A non-financial reference assigned to each Visa payment account that uniquely identifies that payment account and links activity related to that underlying payment account. ID# 0030036 Edition: Apr 2020 | Last Updated: Oct 2017
Payment Application	A software application contained within a Chip or payment data encoded on a Magnetic Stripe that defines the parameters for processing a Transaction. ID# 0024933 Edition: Apr 2020 | Last Updated: Apr 2010
Payment Card Industry Data Security Standard (PCI DSS)	A set of comprehensive requirements that define the standard of due care for protecting sensitive Cardholder information. ID# 0024934 Edition: Apr 2020 | Last Updated: Apr 2010
Payment Card Industry Payment Application Data Security Standard (PA-DSS)	A data security standard that specifies security requirements for third-party Payment Application software that stores, processes, or transmits Cardholder data. ID# 0024935 Edition: Apr 2020 | Last Updated: Oct 2012
Payment Credential	A number or other credential that identifies an account of a Cardholder for use in a Transaction. ID# 0030658 Edition: Apr 2020 | Last Updated: New
Payment Facilitator	A Third Party Agent or non-Member VisaNet Processor that deposits Transactions, receives settlement from or contracts with an Acquirer on behalf of a Sponsored Merchant, and is classified as a Payment Facilitator as specified in *Section 5.3.2.2, Qualification as a Marketplace, Merchant, Payment Facilitator, or Staged Digital Wallet Operator.* ID# 0028921 Edition: Apr 2020 | Last Updated: Apr 2015
Payment Facilitator Agreement	An agreement between a Payment Facilitator and an Acquirer containing their respective rights, duties, and obligations for participation in the Acquirer's Visa Program.

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

	ID# 0026430 Edition: Apr 2020 | Last Updated: Oct 2014
Payment Services Directive (PSD) – Europe Region	The European Parliament and Council directive 2007/64/EC and any subsequent changes.
	ID# 0029731 Edition: Apr 2020 | Last Updated: Oct 2016
Personal Data – Europe Region	Information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person
	ID# 0030567 Edition: Apr 2020 | Last Updated: Apr 2018
Pickup Response	An Authorization Response where the Transaction is declined and confiscation of the Card is requested.
	ID# 0024945 Edition: Apr 2020 | Last Updated: Apr 2010
PIN	A personal identification alpha or numeric code that identifies a Cardholder in an Authorization Request originating at a Terminal with electronic capability.
	ID# 0024948 Edition: Apr 2020 | Last Updated: Apr 2010
PIN Entry Device (PED) – Europe Region	A device used for secure PIN entry and processing, as specified in the *Payment Card Industry PED Security Requirements*.
	ID# 0029732 Edition: Apr 2020 | Last Updated: Oct 2016
PIN Management Requirements Documents	A suite of PIN security documents that includes: • *Payment Card Industry (PCI) – PIN Security Requirements* • *Payment Card Industry (PCI) PIN Transaction Security (PTS) – Point of Interaction (POI) Modular Security Requirements*
	ID# 0027348 Edition: Apr 2020 | Last Updated: Apr 2016
PIN Verification	A procedure used to verify Cardholder identity when a PIN is used in an Authorization Request.
	ID# 0024951 Edition: Apr 2020 | Last Updated: Apr 2010
PIN Verification Service	A service that Visa provides for the verification of Cardholder PINs transmitted with Authorization Requests.

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	ID# 0024953	Edition: Apr 2020 | Last Updated: Apr 2010
PIN Verification Value	A 4-digit value derived with an algorithm using portions of the Account Number, PIN, and a single digit key indicator that is encoded for PIN verification on a Magnetic Stripe or a Chip.	
	ID# 0024954	Edition: Apr 2020 | Last Updated: Apr 2020
PIN-Authenticated Visa Debit Transaction – US Region	A PIN-authenticated Transaction completed at the point of sale with a Visa Debit Card or a Visa Business Check Card in a Card-Present Environment.	
	ID# 0026511	Edition: Apr 2020 | Last Updated: Oct 2014
PIN-Preferring Chip Card	An EMV-Compliant and VIS-Compliant Chip Card containing a Smart Payment Application, and a Cardholder Verification Method list specifying a preference for a PIN-based Cardholder Verification Method (either offline or online).	
	ID# 0024947	Edition: Apr 2020 | Last Updated: Apr 2020
Plus ATM	An ATM that displays the Plus Symbol and not the Visa Brand Mark.	
	ID# 0024956	Edition: Apr 2020 | Last Updated: Apr 2010
Plus Card	A card that bears the Plus Symbol.	
	ID# 0024958	Edition: Apr 2020 | Last Updated: Oct 2015
Plus Program	A program through which a Plus participant provides ATM services to Cardholders by acting as an Issuer, an ATM Acquirer, or both.	
	ID# 0024962	Edition: Apr 2020 | Last Updated: Apr 2010
Plus Program Marks	The Marks used in connection with the Plus Program, including the Diamond Design, Plus Symbol, Plus wordmark, Plus Symbol-Contained, and Plus Symbol-Uncontained, as specified in the *Visa Product Brand Standards.*	
	ID# 0024964	Edition: Apr 2020 | Last Updated: Oct 2015
Plus Symbol	The Visa-Owned Mark that represents the Plus Program and that complies with the specifications in the *Visa Product Brand Standards*.	
	ID# 0024966	Edition: Apr 2020 | Last Updated: Oct 2016
Plus System, Inc.	A subsidiary of Visa U.S.A. Inc. sublicensed to administer the Plus Program in the United States and certain other countries, in accordance	

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	with the affiliation agreements between that entity and Visa.
	ID# 0024969 Edition: Apr 2020 | Last Updated: Apr 2010
Point-of-Sale Balance Inquiry	A Cardholder request for a Prepaid Card account balance that is initiated at the Point-of-Transaction and processed as a separate, non-financial transaction.
	ID# 0025553 Edition: Apr 2020 | Last Updated: Apr 2020
Point-of-Sale Balance Return	An Authorization Response in which an Issuer of Prepaid Cards provides the remaining balance for participating Merchants to print on the Transaction Receipt.
	ID# 0025554 Edition: Apr 2020 | Last Updated: Apr 2020
Point of Transaction	The physical location or online address where a Merchant or Acquirer completes a Transaction.
	ID# 0024974 Edition: Apr 2020 | Last Updated: Oct 2015
Point-of-Transaction Capability – Europe Region	The capability of a Merchant, Acquirer, or Unattended Cardholder-Activated Terminal to process electronic data, obtain an Authorization, and provide Transaction Receipt data.
	ID# 0029733 Edition: Apr 2020 | Last Updated: Oct 2016
POS	Point of sale.
	ID# 0029311 Edition: Apr 2020 | Last Updated: Oct 2016
POS Entry Mode	An International Organization for Standardization-defined Authorization or Online Financial Transaction field indicating the method used to obtain and transmit the Cardholder information necessary to complete a Transaction (for example: manual key entry, Magnetic-Stripe read, Chip-read).
	ID# 0024990 Edition: Apr 2020 | Last Updated: Oct 2016
Post-Issuance Application Change – Europe Region	A method that enables an Issuer to modify or block an application already residing on a Chip.
	ID# 0029734 Edition: Apr 2020 | Last Updated: Oct 2016
Post-Issuance Application Load – Europe Region	A method that enables an Issuer to add an application or service to the contents of a Chip without reissuing a Card.
	ID# 0029735 Edition: Apr 2020 | Last Updated: Oct 2016

Glossary
Glossary
Visa Core Rules and Visa Product and Service Rules

Post-Issuance Updates	A method that enables an Issuer to do either of the following without requiring reissuance of a Chip Card: • Add an application or service to a Chip (in the Europe Region, Post-Issuance Application Load) • Modify or block an existing application on a Chip (in the Europe Region, Post-Issuance Application Change) ID# 0024987 ⎮ Edition: Apr 2020 ⎮ Last Updated: Oct 2016
Preauthorized Health Care Transaction – US Region	A Transaction completed by a Health Care Merchant for which a Cardholder has provided written permission to the Merchant to charge the Cardholder's Visa account for services. ID# 0024991 ⎮ Edition: Apr 2020 ⎮ Last Updated: Oct 2014
Preauthorized Payment Cancellation Service	**Effective through 16 August 2020 in the Europe Region, effective through 18 October 2020 in the AP Region, Canada Region, CEMEA Region, LAC Region, and effective through 16 April 2021 in the US Region** A service that enables Issuers to stop payment on preauthorized Transactions. ID# 0026230 ⎮ Edition: Apr 2020 ⎮ Last Updated: Apr 2020
Prepaid Account	An account established by an Issuer, with previously deposited, authorized, or transferred funds, which is decreased by purchase Transactions, Cash Disbursements, or account fees. ID# 0024994 ⎮ Edition: Apr 2020 ⎮ Last Updated: Apr 2010
Prepaid Card	A Card linked to a reloadable or non-reloadable pre-funded account, or a Prepaid Account or equivalent as defined under applicable laws or regulations. ID# 0024996 ⎮ Edition: Apr 2020 ⎮ Last Updated: Apr 2020
Prepaid Clearinghouse Service	A centralized database that consolidates, tracks, and aggregates Prepaid Card enrollments, Load Transactions, reloads, unauthorized Transaction requests, and fraud, for use in identifying and mitigating fraud within the lifecycle of a Prepaid Account. ID# 0029068 ⎮ Edition: Apr 2020 ⎮ Last Updated: Apr 2020
Prepaid Partner	A Merchant, Member, or Third Party Agent that has a contract with an Issuer or Acquirer to sell, activate, and/or perform Load Transaction processing for Prepaid Cards.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0024998 Edition: Apr 2020 | Last Updated: Apr 2020
Prepaid Partner Agreement	A contract between a Prepaid Card Issuer or Acquirer and a Member, Merchant, or Third Party Agent containing respective rights, duties, and obligations for the sale, activation, and/or Load Transaction processing of Prepaid Cards.
	ID# 0024999 Edition: Apr 2020 | Last Updated: Apr 2020
Presentment	A Clearing Record that an Acquirer presents to an Issuer through Interchange, either initially (a first Presentment) or after a Dispute (a Dispute Response or pre-Arbitration).
	ID# 0025001 Edition: Apr 2020 | Last Updated: Apr 2018
Primary Mark	A Visa-Owned Mark on a Card that identifies the primary Payment Credential when multiple Brand Marks (including both Visa-Owned and Non-Visa-Owned Marks) are contained on a Chip Card.
	ID# 0025004 Edition: Apr 2020 | Last Updated: Apr 2020
Principal Place of Business	The fixed location at which a Merchant's or Payment Facilitator's executive officers direct, control, and coordinate the entity's activities.
	ID# 0029549 Edition: Apr 2020 | Last Updated: Apr 2017
Principal-Type Member	A Member of Visa characterized as one of the following: • Principal Member, as defined in the Visa Charter Documents • Acquirer Member, as defined in the applicable Visa Charter Documents • Administrator Member, as defined in the Visa U.S.A. Inc. Certificate of Incorporation and By-Laws, Article II, Section 2.04(c) • Group Member, as defined in the applicable Visa Charter Documents • Merchant Acquirer Member, as defined in the applicable Visa Charter Documents • Cash Disbursement Member, as defined in the applicable Visa Charter Documents
	ID# 0025005 Edition: Apr 2020 | Last Updated: Apr 2018
Private Agreement	A bilateral agreement between Members, or the operating regulations of a Group Member, pertaining to Authorization or Clearing and

	Glossary	

Glossary

Visa Core Rules and Visa Product and Service Rules

	Settlement of Domestic Transactions. **ID# 0025013** Edition: Apr 2020 | Last Updated: Apr 2010
Private Arrangement	In the Canada Region, US Region: An agreement where Authorization Requests or Transactions involving 2 different Members are not processed through VisaNet. Private Arrangements are prohibited. **ID# 0025014** Edition: Apr 2020 | Last Updated: Apr 2017
Private Label Card	A merchant's proprietary card that is accepted only at its own locations, or a multi-use non-Visa-branded Card. **ID# 0025016** Edition: Apr 2020 | Last Updated: Oct 2011
Privately Contracted Agreement – Europe Region	An agreement between an Issuer of Visa Drive Cards that are "extra" Cards and a Merchant that is not part of a Closed Loop, under which the Merchant agrees to accept and process Transactions on Visa Drive Cards that are "extra" Cards. **ID# 0029736** Edition: Apr 2020 | Last Updated: Oct 2016
Processing Date	The date (based on Greenwich Mean Time) on which the Member submitted, and Visa accepted, Interchange data. Equivalents to the Processing Date are: • In BASE II, the central processing date • In the Single Message System, the Settlement Date (for financial Transactions) or date the Transaction is entered into the Single Message System (for non-financial Transactions) • If cleared under a Private Agreement, the date on which a Member processes outgoing Interchange • Endorsement date, if the Interchange data was accepted by Visa on the same date on which it was first submitted by the Acquirer • The date on which Visa accepted an action processed through Visa Resolve Online (VROL) **ID# 0025017** Edition: Apr 2020 | Last Updated: Apr 2016
Product Category – Europe Region	Any of the following: • Debit • Credit • Commercial

<table>
<tr><td colspan="2" align="center">**Glossary**</td></tr>
</table>

Visa Core Rules and Visa Product and Service Rules

	• Prepaid
	ID# 0029738 Edition: Apr 2020 | Last Updated: Oct 2016
Proprietary Card	A Card that does not bear the Visa Brand Mark or Visa Brand Mark with the Electron Identifier, but may be either or both:
	• Plus-enabled
	• Interlink-enabled
	ID# 0025020 Edition: Apr 2020 | Last Updated: Apr 2017
Proprietary Network	A network owned and operated by a single Plus ATM Member that passes Transactions between its network and other networks, but operates all of the ATMs in its network.
	ID# 0030602 Edition: Apr 2020 | Last Updated: Apr 2019
Public Key	The non-secret portion of the cryptographic method used for verification during a Transaction.
	ID# 0025028 Edition: Apr 2020 | Last Updated: Oct 2014
Q	
Qualifying Purchase – US Region	A purchase Transaction completed with a Visa Traditional Rewards Card that an Issuer may consider for the purpose of awarding Rewards Currency. An Issuer may exclude the following Transactions from qualifying:
	• Balance transfers
	• Convenience checks
	• Cash Disbursements
	• Finance charges
	• Quasi-Cash Transactions
	• Any Transaction not authorized by the Cardholder
	ID# 0025031 Edition: Apr 2020 | Last Updated: Oct 2014
Quasi-Cash Transaction	A Transaction representing a Merchant's or Member's sale of items that are directly convertible to cash, such as:
	• Gaming chips
	• Money orders

Glossary	

Glossary

Visa Core Rules and Visa Product and Service Rules

	- Deposits - Wire Transfers - Travelers cheques - Prepaid Cards with cash access - Foreign currency - Additional Transactions approved by Visa ID# 0025033 Edition: Apr 2020 | Last Updated: Apr 2020
R	
Real-Time Clearing	A program for Acquirers and Merchants that allows an Automated Fuel Dispenser Merchant to send through the Single Message System an Authorization Request for an amount that may differ from the Transaction amount. ID# 0025034 Edition: Apr 2020 | Last Updated: Oct 2017
Receiving Member	A Member receiving a Transaction through Interchange. ID# 0025038 Edition: Apr 2020 | Last Updated: Apr 2010
Recipient Issuer	An Issuer that receives an Original Credit Transaction. ID# 0025039 Edition: Apr 2020 | Last Updated: Oct 2018
Recurring Transaction	A Transaction in a series of Transactions that use a Stored Credential and that are processed at fixed, regular intervals (not to exceed one year between Transactions), representing Cardholder agreement for the Merchant to initiate future Transactions for the purchase of goods or services provided at regular intervals. ID# 0025041 Edition: Apr 2020 | Last Updated: Oct 2017
Reference Card	An item containing relevant account information, such as a Payment Credential or expiration date, that is provided to a Virtual Account owner. ID# 0025043 Edition: Apr 2020 | Last Updated: Apr 2020
Registered Program Identification Number	A number assigned by an Issuer for the purpose of identifying and tracking any rewards program offered in connection with the Issuer's Card products. ID# 0025587 Edition: Apr 2020 | Last Updated: Oct 2014

Glossary	

<div align="center">Glossary</div>

<div align="center">Visa Core Rules and Visa Product and Service Rules</div>

Reloadable Prepaid Card	A Prepaid Card that may be funded more than once.
	ID# 0025059 Edition: Apr 2020 | Last Updated: Apr 2020
Retail Merchant	A Merchant that is not one of the following: • Mail/Phone Order Merchant • Merchant that processes Recurring Transactions for the sale of recurring services • T&E Merchant (except in the Europe Region)
	ID# 0025068 Edition: Apr 2020 | Last Updated: Oct 2016
Retail Transaction	A Transaction at a Retail Merchant outlet.
	ID# 0025069 Edition: Apr 2020 | Last Updated: Apr 2010
Retrieval Request	An Issuer's request for a Transaction Receipt, which could include the original, a paper copy or facsimile, or an electronic version thereof.
	ID# 0025070 Edition: Apr 2020 | Last Updated: Apr 2010
Reversal	A Deferred Clearing or Online Financial Transaction used to negate or cancel a transaction that has been sent through Interchange in error.
	ID# 0025072 Edition: Apr 2020 | Last Updated: Oct 2016
Rewards Currency – US Region	A reward denomination defined by an Issuer consisting of air miles, points, or discounts offered in connection with a Visa Traditional Rewards Card.
	ID# 0025073 Edition: Apr 2020 | Last Updated: Oct 2014
S	
Sample Card Design	A background design provided by Visa that is unique for each Card product and that an Issuer may use on the front of a Card.
	ID# 0025077 Edition: Apr 2020 | Last Updated: Apr 2020
Scrip	A 2-part paper receipt that is redeemable at a Merchant Outlet for goods, services, or cash.
	ID# 0025079 Edition: Apr 2020 | Last Updated: Apr 2010
Secure Electronic Commerce Transaction	An Electronic Commerce Transaction that has been authenticated using an Authentication Method.

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	ID# 0025084 Edition: Apr 2020 | Last Updated: Oct 2019
Secured Card – AP Region	A Card for which the Issuer requires a cash deposit as collateral before issuing the Card.
	ID# 0029453 Edition: Apr 2020 | Last Updated: Apr 2020
Sending Member	A Member entering a Transaction into Interchange.
	ID# 0025092 Edition: Apr 2020 | Last Updated: Apr 2010
Service Code	A valid sequence of digits recognized by VisaNet that is encoded on a Magnetic Stripe and replicated on the Magnetic-Stripe Image in a Chip that identifies the circumstances under which the Card is valid (for example: International Transactions, Domestic Transactions, restricted Card use), and defines requirements for processing a Transaction with the Card (for example: Chip-enabled, Cardholder Verification, Online Authorization).
	ID# 0025094 Edition: Apr 2020 | Last Updated: Oct 2014
Service Fee	A fee assessed to a Cardholder that uses a Card to pay for goods and services in a permitted Merchant category.
	ID# 0030125 Edition: Apr 2020 | Last Updated: Apr 2020
Settlement	The reporting and funds transfer of Settlement Amounts owed by one Member to another, or to Visa, as a result of Clearing.
	ID# 0025095 Edition: Apr 2020 | Last Updated: Apr 2011
Settlement Amount	The daily net amounts expressed in a Member's Settlement Currency resulting from Clearing. These amounts include Transaction and Fee Collection Transaction totals, expressed in a Member's Settlement Currency.
	ID# 0025096 Edition: Apr 2020 | Last Updated: Apr 2011
Settlement Bank	A bank, including a Correspondent Bank or Intermediary Bank, that is both: • Located in the country where a Member's Settlement Currency is the local currency • Authorized to execute Settlement of Interchange on behalf of the Member or the Member's bank

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

ID# 0025097	Edition: Apr 2020 | Last Updated: Oct 2014
Settlement Currency	A currency that Visa uses to settle Interchange.
ID# 0025098	Edition: Apr 2020 | Last Updated: Oct 2016
Settlement Date	The date on which Visa initiates the transfer of Settlement Amounts in the Settlement of Interchange. See Processing Date.
ID# 0025099	Edition: Apr 2020 | Last Updated: Apr 2010
Settlement Loss – Europe Region	The amounts actually payable by one Member to another Member pursuant to the provisions of any drafts or other instruments processed in accordance with the Visa Rules and not any consequential damages or expenses incurred in attempting to settle such drafts or other instruments, or any interest expenses, whether actually incurred or imputed, associated with delays in settlement.
ID# 0029743	Edition: Apr 2020 | Last Updated: Oct 2016
Settlement Reporting Entity	A name or number of an entity assigned by Visa and authorized by the Member that is used by Visa for Settlement reporting.
ID# 0026049	Edition: Apr 2020 | Last Updated: Oct 2019
Settlement Service	A service that allows Members to consolidate the Settlement functions of the Visa systems into one centralized function and benefit from flexible reporting options.
ID# 0029744	Edition: Apr 2020 | Last Updated: Oct 2016
Shared Deposit	The switching of ATM deposit Transactions between Plus ATM Members.
ID# 0030607	Edition: Apr 2020 | Last Updated: Apr 2019
Shared Deposit Service	An optional service that supports switching of Plus ATM deposit Transactions between Members. This service allows Cardholders of participating Issuers to perform Shared Deposit Transactions at participating Acquirers' ATMs.
ID# 0030606	Edition: Apr 2020 | Last Updated: Apr 2019
SIGIS – US Region	An industry trade group, known as the Special Interest Group for Inventory Information Approval System (IIAS) Standards, chartered with implementing processing standards for Healthcare Auto-Substantiation Transactions in accordance with Internal Revenue Service (IRS)

	regulations and responsible for licensing and certifying Merchants, Members, and Agents that process such Transactions.
	ID# 0025102 Edition: Apr 2020 | Last Updated: Oct 2014
Single Message System	A service that processes Online Financial and Deferred Clearing Transactions through a single VisaNet interface for purchases and ATM Transactions.
	ID# 0025108 Edition: Apr 2020 | Last Updated: Oct 2016
Sponsor	A Member or Non-Member Administrator that is responsible, in part or whole, for other Members of Visa, as specified in the applicable Visa Charter Documents.
	ID# 0025120 Edition: Apr 2020 | Last Updated: Apr 2016
Sponsored Member	A Member of Visa whose right to participate in Visa is dependent upon another Member, as specified in the applicable Visa Charter Documents. A Member of the Canada Region or US Region whose right to participate in Visa is dependent upon sponsorship of another Member, as specified in *Appendix E* to the *Canada Regional Operating Regulations* and the *Visa U.S.A. Inc. Certificate of Incorporation and By-Laws*, Article II.
	ID# 0025118 Edition: Apr 2020 | Last Updated: Oct 2016
Sponsored Merchant	An entity for which Visa payment services are provided by a Payment Facilitator.
	ID# 0025119 Edition: Apr 2020 | Last Updated: Apr 2015
Sponsorship Marks	The Marks of an entity with which Visa has entered into an agreement to act as a sponsor for that entity's activities or events.
	ID# 0026242 Edition: Apr 2020 | Last Updated: Apr 2011

Staged Digital Wallet	Functionality provided by a Digital Wallet Operator (DWO) that does all of the following:
	
	 • Can be used at more than one retailer
	 • Uses both:
	   – A Payment Credential
	   – A separate account or accounts assigned by the DWO to the

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

<table>
<tr>
<td></td>
<td>Cardholder
Is used by the Staged Digital Wallet Operator to complete a Transaction, in any order, as follows:
– Purchase: pays the retailer using the account assigned by the DWO
– Funding: uses the Payment Credential to fund or reimburse the Staged Digital Wallet. The DWO deposits the Transaction for the funding amount with its Acquirer using the Payment Credential.
Is capable of a purchase with back-to-back funding, (also known as liveload), where the funding Transaction both:
– Is initiated by the SDWO
– Corresponds to, or is otherwise directly connected to a specific purchase. The amount funded from the Payment Credential may represent the whole or a part of the purchase price and consist of one or more funding Transactions.

ID# 0029532   Edition: Apr 2020 | Last Updated: Apr 2020</td>
</tr>
<tr>
<td>Staged Digital Wallet Operator (SDWO)</td>
<td>A Digital Wallet Operator that operates a Staged Digital Wallet.

ID# 0029531   Edition: Apr 2020 | Last Updated: Oct 2017</td>
</tr>
<tr>
<td>Stand-In Processing (STIP)</td>
<td>The component that provides Authorization services on behalf of an Issuer when the Positive Cardholder Authorization System is used or when the Issuer, its VisaNet Processor, or a Visa Scheme Processor is unavailable.

ID# 0025121   Edition: Apr 2020 | Last Updated: Oct 2016</td>
</tr>
<tr>
<td>Stand-In Processing Account</td>
<td>An Issuer-supplied valid Account Number (established and activated in the Issuer's Authorization system) that is securely maintained by Visa Global Customer Care Services and used for Emergency Cash Disbursements and Emergency Card Replacements.

ID# 0025122   Edition: Apr 2020 | Last Updated: Apr 2019</td>
</tr>
<tr>
<td>Status Check Authorization</td>
<td>An Authorization Request for one currency unit submitted by an Automated Fuel Dispenser Merchant.

ID# 0025130   Edition: Apr 2020 | Last Updated: Apr 2016</td>
</tr>
<tr>
<td>Stop Payment Service</td>
<td>Effective 17 August 2020 in the Europe Region, and effective 19</td>
</tr>
</table>

	Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	October 2020 in the AP Region, Canada Region, CEMEA Region, LAC Region, US Region A service that allows an Issuer, upon Cardholder request, to place a stop instruction against a Transaction completed in a Card-Absent Environment.
	ID# 0030697 · Edition: Apr 2020 | Last Updated: New
Stored Credential	Information (including, but not limited to, a Payment Credential) that is stored by a Merchant or its agent, a Payment Facilitator, or a Staged Digital Wallet Operator to process future Transactions.
	ID# 0029547 · Edition: Apr 2020 | Last Updated: Apr 2020
Strategic Bankruptcy Solutions – US Region	A Visa service that does all of the following: • Identifies Cardholders, cardholders of non-Visa cards, customers of other Visa or non-Visa products, and applicants for Cards, non-Visa cards, and other Visa or non-Visa products who have filed bankruptcy • Files claims and documents on behalf of Members with the bankruptcy courts • Assists Members in assessing the value of obligations of Cardholders and other individuals who have declared bankruptcy
	ID# 0025133 · Edition: Apr 2020 | Last Updated: Oct 2014
Strong Customer Authentication Delegate – Europe Region	In the Europe Region: An entity enrolled in the Delegated Authentication Program to provide strong customer authentication on behalf of Issuers.
	ID# 0030623 · Edition: Apr 2020 | Last Updated: Apr 2019
Summary of Interchange Entries	Data required to accompany domestic Interchange processed under a Private Agreement.
	ID# 0029745 · Edition: Apr 2020 | Last Updated: Oct 2016
Surcharge – AP Region	A fee assessed to a Cardholder by a Merchant in Australia that is added to a Transaction for the acceptance of a Card.
	ID# 0027588 · Edition: Apr 2020 | Last Updated: Apr 2020
T	
T&E	Travel and entertainment. All of the following Merchants and Merchant segments:

Glossary	

Visa Core Rules and Visa Product and Service Rules

	- Airlines - Cruise Lines - Lodging Merchants - Passenger railways located in the US Region - Travel agencies - Vehicle Rental Merchants ID# 0025141 Edition: Apr 2020 | Last Updated: Apr 2018
Telephone Service Transaction	A Transaction in which a Cardholder uses a Card to purchase a telephone call. ID# 0025153 Edition: Apr 2020 | Last Updated: Apr 2020
Terminal Risk Management	A process performed by a Chip-Reading Device to protect a Member from fraud by: - Initiating Online Issuer Authorization for above-Floor Limit Transactions - Ensuring random Online processing for below-Floor Limit Transactions - Performing Transaction velocity checking ID# 0025154 Edition: Apr 2020 | Last Updated: Apr 2010
Terminated Merchant File – US Region	A file (currently known as "MATCH") maintained by MasterCard Worldwide that identifies Merchants and principals of Merchants that Acquirers have terminated for specified reasons. ID# 0025159 Edition: Apr 2020 | Last Updated: Oct 2014
Third Party Agent	An entity, not defined as a VisaNet Processor or Visa Scheme Processor, that provides payment-related services, directly or indirectly, to a Member and/or its Merchants or Sponsored Merchants or their agents. ID# 0025921 Edition: Apr 2020 | Last Updated: Apr 2020
Third-Party Personalizer	A third party that Visa certifies or approves to personalize Cards for Issuers. ID# 0029746 Edition: Apr 2020 | Last Updated: Oct 2016
Token	A type of Payment Credential issued in accordance with the *EMV Payment Tokenisation Specification – Technical Framework*.

Glossary	
	Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0029108 Edition: Apr 2020 | Last Updated: Apr 2020
Token Requestor	An entity registered with a Token Service Provider to initiate requests for payment Tokens in accordance with the *EMV Payment Tokenization Specification*.
	ID# 0029519 Edition: Apr 2020 | Last Updated: Apr 2017
Token Service Provider	An entity that provides a payment Token to a Token Requestor.
	ID# 0029747 Edition: Apr 2020 | Last Updated: Oct 2016
Tracing Data	In a V.I.P. System message, the transmission date and time, systems trace audit number, retrieval reference number, Transaction Identifier, and Acquiring Identifier. See Acquirer Reference Number.
	ID# 0025170 Edition: Apr 2020 | Last Updated: Oct 2019
Trade Name	A name used to identify a business and to distinguish its activities from those of other businesses. In some cases, the same words or symbols may serve as a Trade Name and Mark simultaneously.
	ID# 0025172 Edition: Apr 2020 | Last Updated: Apr 2010
Trailing Dispute Activity	Dispute activity at a Merchant Outlet that occurs after an Acquirer has stopped processing sales Transactions for the Merchant.
	ID# 0030555 Edition: Apr 2020 | Last Updated: Apr 2018
Transaction	The use of a Payment Credential to make a payment or otherwise exchange value between a Cardholder (or an Issuer) and a Merchant (or an Acquirer).
	ID# 0025175 Edition: Apr 2020 | Last Updated: Apr 2020
Transaction Country	The country in which a Merchant Outlet is located.
	ID# 0025179 Edition: Apr 2020 | Last Updated: Oct 2016
Transaction Currency	The fiat currency in which a Transaction is completed.
	ID# 0025180 Edition: Apr 2020 | Last Updated: Apr 2018
Transaction Date	The date on which a Transaction between a Cardholder and a Merchant or an Acquirer occurs.
	ID# 0025181 Edition: Apr 2020 | Last Updated: Apr 2010

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Transaction Identifier	A unique value assigned to each Transaction and returned to the Acquirer in the Authorization Response. Visa uses this value to maintain an audit trail throughout the life cycle of the Transaction and all related transactions, such as Reversals, Adjustments, confirmations, and Disputes.
	ID# 0025182 Edition: Apr 2020 | Last Updated: Apr 2018
Transaction Information	Information necessary for processing Transactions, as specified in the *Payment Card Industry Data Security Standard (PCI DSS).*
	ID# 0025183 Edition: Apr 2020 | Last Updated: Oct 2014
Transaction Receipt	An electronic or paper record of a Transaction (or a copy), generated at the Point-of-Transaction.
	ID# 0025184 Edition: Apr 2020 | Last Updated: Apr 2011
Travel Period	A fixed period of time within which a Mass Transit Merchant accumulates journey data for a Cardholder using their transit network.
	ID# 0030052 Edition: Apr 2020 | Last Updated: Apr 2018
Trusted Beneficiary – Europe Region	In the Europe Region: An entity listed as trusted by a Cardholder in line with applicable regulation.
	ID# 0030624 Edition: Apr 2020 | Last Updated: Apr 2019
Trusted Listing Program – Europe Region	In the Europe Region: A Visa program that supports a Cardholder in confirming, to its Issuer, a Trusted Beneficiary, in line with applicable regulation.
	ID# 0030625 Edition: Apr 2020 | Last Updated: Apr 2019
U	
Unable-to-Authenticate Response	A message from a Visa Secure Issuer in response to an Authentication Request indicating that the Issuer is unable to authenticate the Cardholder for reasons other than those that result in an Authentication Denial.
	ID# 0025194 Edition: Apr 2020 | Last Updated: Apr 2019
Unattended Cardholder-Activated Terminal	An Acceptance Device that dispenses goods and/or provides services under all of the following conditions: • Card is present • Cardholder is present

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

	• Individual representing the Merchant or Acquirer is not physically present
	• Authorization, if required is obtained electronically
	ID# 0025720 Edition: Apr 2020 | Last Updated: Oct 2015
Unattended Transaction	A Transaction conducted at an Unattended Cardholder-Activated Terminal.
	ID# 0025721 Edition: Apr 2020 | Last Updated: Oct 2012
Unauthorized Use	A Transaction that meets one of the following criteria: • Is not processed on behalf of a Member • Is processed on behalf of a Member by a VisaNet Processor or Visa Scheme Processor not designated for processing activities • Is processed on behalf of a Member but not within the scope of the Member's category or categories of membership • Is not within the scope of activities approved by the Member, the Member's Sponsor, or Visa • Is processed using a BIN or an Acquiring Identifier that has not been designated by the BIN Licensee or Acquiring Identifier Licensee for that Member's use
	ID# 0025922 Edition: Apr 2020 | Last Updated: Oct 2019
Unscheduled Credential-on-File Transaction	A Transaction using a Stored Credential for a fixed or variable amount that does not occur on a scheduled or regularly occurring Transaction Date, where the Cardholder has provided consent for the Merchant to initiate one or more future Transactions.
	ID# 0029548 Edition: Apr 2020 | Last Updated: Oct 2017
US Covered Visa Debit Card – US Region and US Territories	A Card issued in the US Region or a US Territory that accesses a transaction, savings, or other asset account, regardless of whether Cardholder Verification is based on signature, PIN, or other means, including a general-use Prepaid Card and Consumer Visa Deferred Debit Card, but solely to the extent any such Card is a "debit card" as defined in Federal Reserve Board Regulation II, 12 CFR Part 235.
	ID# 0026512 Edition: Apr 2020 | Last Updated: Apr 2020
US Credit Card Surcharge – US Region and US	A fee assessed to a Cardholder by a Merchant in the US Region or a US Territory that is added to a Credit Card Transaction for the acceptance

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Territories	of a Credit Card.
	ID# 0027533 Edition: Apr 2020 | Last Updated: Apr 2020
US Domestic Transaction	A Transaction that occurs inside one of the following: • The 50 United States, including the District of Columbia • A US military base overseas • A US embassy or consulate on foreign territory ID# 0003684 Edition: Apr 2020 | Last Updated: Apr 2019
US Territory	One of the following: • American Samoa • Guam • Commonwealth of the Northern Mariana Islands • Puerto Rico • US Minor Outlying Islands • US Virgin Islands ID# 0026422 Edition: Apr 2020 | Last Updated: Oct 2014
V	
V Distribution Program	An enhanced Visa Business Card or Visa Purchasing Card program that enables wholesale and retail Merchants to use a Visa product to pay for goods and services in a business-to-business setting. ID# 0025419 Edition: Apr 2020 | Last Updated: Oct 2015
V.I.P. System	The processing component of the VisaNet Integrated Payment System comprised of BASE I and the Single Message System used for single message Authorization in connection with financial Transaction processing. ID# 0025201 Edition: Apr 2020 | Last Updated: Apr 2010
Vehicle Rental Merchant	A Merchant that rents cars, vans, trucks, trailers, and other similar vehicles (MCCs 3351 – 3500, 7512, 7513). ID# 0029520 Edition: Apr 2020 | Last Updated: Apr 2018
Vehicle-Specific Fleet Card	A Visa Commercial Card with Visa Fleet service enhancement that is assigned to a specific vehicle and limited to purchases of fuel and

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	vehicle maintenance.
	ID# 0025208 Edition: Apr 2020 | Last Updated: Apr 2019
Verified by Visa	See Visa Secure.
	ID# 0025209 Edition: Apr 2020 | Last Updated: Apr 2019
Virtual Account	Either: • An account established for an individual or a commercial entity primarily for completing Electronic Commerce Transactions and for which no physical Card is required. • For a Visa B2B Virtual Payments Program product, a dynamic Payment Credential generated in connection with a Card-Absent Environment Transaction initiated by a commercial entity. This does not include the accounts established for facilitating Mobile Push Payment Transactions.
	ID# 0025211 Edition: Apr 2020 | Last Updated: Apr 2020
VIS-Compliant	A Card application that complies with either: • The *Visa Integrated Circuit Card Specification (VIS)* and has been approved by Visa Approval Services • In the US Region, a Card application that complies with the Visa Integrated Circuit Card Specification (VIS)
	ID# 0025214 Edition: Apr 2020 | Last Updated: Apr 2017
Visa	Visa International Service Association and all of its subsidiaries and affiliates, and subsidiaries and affiliates of Visa Inc. When used within the Visa Rules, Visa refers to any Visa Inc. subsidiary, affiliate, regional office, management, or committee as applicable.
	ID# 0025217 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Advanced ID Solutions – US Region	A Visa service that is designed to reduce Member credit and fraud losses related to Card, non-Visa card, and other Visa and non-Visa products through the use of the Issuers' Clearinghouse Service, the Visa ICS Prescreen Service, and ID Analytics, Inc. services (ID Score Plus and Credit Optics).
	ID# 0025239 Edition: Apr 2020 | Last Updated: Oct 2014
Visa Agro Card – LAC	A Card issued to commercial entities in the public and private sector

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Region	for commercial purchases associated with the agribusiness sector. ID# 0026526 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Alerts Service (VAS) – Europe Region	The Alert processing service provided by Visa to Issuers consisting of the Visa Alerts Data Feed Service. ID# 0029753 Edition: Apr 2020 | Last Updated: Oct 2016
Visa ATM	An ATM that displays the Visa Brand Mark or the Visa Flag Symbol, but not the Plus Symbol. ID# 0025241 Edition: Apr 2020 | Last Updated: Apr 2010
Visa Brand Mark	A Visa-Owned Mark that represents the Visa organization and its product and service offerings. ID# 0025245 Edition: Apr 2020 | Last Updated: Apr 2018
Visa Brand Mark with the Electron Identifier	A Visa-Owned Mark consisting of the Visa Brand Mark and the name "Electron." ID# 0025246 Edition: Apr 2020 | Last Updated: Oct 2013
Visa Business Card	A Card issued to employees or sole proprietors of small businesses for the payment of employees' business travel and general business expenses. This does not apply in the US Region to Visa Business Check Cards used to pay Debt. ID# 0025248 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Business Check Card – US Region	A Visa Business Card issued as a Visa Check Card. ID# 0025250 Edition: Apr 2020 | Last Updated: Oct 2014
Visa Business Debit Card – Canada Region	A Card that accesses a business deposit account or equivalent account, excluding Prepaid Cards and Prepaid Accounts. ID# 0027282 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Business Electron Card	A Visa Electron Card intended for the small business market and used to pay for employee business travel and general business expenses. ID# 0025252 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Buxx – US Region	A Prepaid Card designed for teenagers, with account ownership by a parent or guardian.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0025255 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Canada	Visa Canada Corporation.
	ID# 0025257 Edition: Apr 2020 | Last Updated: Apr 2010
Visa Card	A Card that bears the Visa Brand Mark.
	ID# 0025258 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Cargo Card – LAC Region	A Visa Commercial Card targeted to carriers/shippers' service providers to pay for truck drivers' expenses related to the transportation business. A Visa Cargo Card is either of the following: • Visa Commercial Prepaid Product • Visa Business Electron Card
	ID# 0026071 Edition: Apr 2020 | Last Updated: Oct 2015
Visa Cash-Back Service	A service whereby cash may be obtained from a qualifying Merchant through use of a Card in conjunction with, and processed as, a domestic Retail Transaction. In the Europe Region: The Cash-Back Service. In the US Region: The service is accessed with a Debit Card or Visa Business Check Card and processed as a PIN-Authenticated Visa Debit Transaction.
	ID# 0026046 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Central Travel Account	A Virtual Account or a Payment Credential that an Issuer assigns to a commercial entity using a Visa Corporate Card BIN or Visa Purchasing Card BIN that is generally used for travel-related purchases.
	ID# 0026400 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Charge Card – AP Region and US Region	A type of Visa Consumer Credit Card that is non-revolving and requires the total outstanding balance to be paid in full each statement cycle.
	ID# 0026358 Edition: Apr 2020 | Last Updated: Apr 2016
Visa Check Card – US Region	A Consumer Visa Check Card or Visa Business Check Card that accesses a deposit, investment, or other consumer or business asset account, including a fiduciary account.
	ID# 0025268 Edition: Apr 2020 | Last Updated: Oct 2014

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Visa Checkout	Where available, a Visa platform that enables a Visa Checkout Account Holder to store and manage accounts in a secure centralized location, make purchases with Visa Checkout Merchants, and use other forms of financial and non-financial services.
	ID# 0026984 Edition: Apr 2020 | Last Updated: Oct 2015
Visa Checkout Account Holder	A user that has successfully enrolled in Visa Checkout. A Visa Checkout Account Holder may or may not be a Cardholder.
	ID# 0026986 Edition: Apr 2020 | Last Updated: Oct 2014
Visa Commercial Cards	A physical or virtual Card intended for business expense use and comprising: • Visa Business Card • Visa Business Electron Card • Visa Corporate Card • Visa Purchasing Card, including Visa Fleet Card • Visa Agro (This only applies in the LAC Region) • V Distribution Program Card
	ID# 0025272 Edition: Apr 2020 | Last Updated: Oct 2015
Visa Commercial Prepaid Product	A Visa Commercial Card product, issued as a Prepaid Card, in which the corporation depositing the funds remains the owner of the funds in the Prepaid Account. Visa Commercial Prepaid Products are offered to client organizations solely to provide a means to pay for the acquisition of business-related goods and services.
	ID# 0024463 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Confidential	A classification label assigned to information created by Visa and shared with Members under non-disclosure agreements, the use and Member handling of which is subject to certain minimum standards of diligence and care to prevent unauthorized disclosure or business harm to Visa.
	ID# 0026799 Edition: Apr 2020 | Last Updated: Apr 2018
Visa Consumer Card	A Card other than a Visa Commercial Card issued to individuals for the purchase of goods and services used for personal consumption.
	ID# 0025276 Edition: Apr 2020 | Last Updated: Apr 2020

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Visa Contactless Application	A Visa application contained on a Chip that enables a *Visa Contactless Payment Specification*-compliant Contactless Payment Transaction to be performed. ID# 0027792 Edition: Apr 2020 | Last Updated: Apr 2018
Visa Corporate Card	A Visa Commercial Card targeted to mid-to-large size companies that is primarily used to pay for employee business travel and entertainment expenses. ID# 0025280 Edition: Apr 2020 | Last Updated: Oct 2015
Visa Corporate Prepaid Card	A Prepaid Card that draws from funds owned by a commercial or government entity in a Prepaid Account that is used primarily to pay for business travel and entertainment expenses. ID# 0026742 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Credit Acceptor – Canada Region	A Merchant that accepts Credit Cards issued by Canadian Issuers. ID# 0025971 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Credit and Business Category – US Region	A Card category that consists of all of the following: • Consumer Card, other than a Debit Card, issued by a US Issuer • Visa Commercial Card product • Card issued by a non-US Issuer ID# 0025283 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Credit Card Cost of Acceptance – US Region and US Territories	In the US Region, US Territory: One of the following: • The average effective Interchange Reimbursement Fee (IRF) rate plus the average of all fees imposed by Visa on the Acquirer or Merchant, expressed as a percentage of the Transaction amount, applicable to Credit Card Transactions at the Merchant for the preceding one or 12 months, at the option of the Merchant • If a Merchant cannot determine its Visa Credit Card Cost of Acceptance, the Credit Card cost of acceptance for the Merchant's category as communicated via the Visa public website, *www.visa.com* ID# 0027535 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Credit Card Product Cost of Acceptance – US	For a Merchant in the US Region or a US Territory, one of the following:

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

Region and US Territories	• The average effective Interchange Reimbursement Fee (IRF) rate plus the average of all fees imposed by Visa on the Acquirer or Merchant, expressed as a percentage of the Transaction amount, applicable to Credit Card Transactions of a product type at the Merchant for the preceding one or 12 months, at the option of the Merchant. • If a Merchant cannot determine its Visa Credit Card Product Cost of Acceptance, the Visa Credit Card product cost of acceptance for the Merchant's category as communicated via the Visa public website, *www.visa.com* ID# 0027536 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Credit Card Surcharge Cap – US Region and US Territories	The average Merchant Discount Rate that a Merchant in the US Region or a US Territory pays to its Acquirer for Credit Card Transactions completed with a specific Visa product type. The average Merchant Discount Rate is either: • Calculated based on Credit Card Transactions conducted by the Merchant for the preceding 12 months • At any given point in time, the actual Merchant Discount Rate paid in the time period covered by the Merchant's most recent statement relating to Credit Card Transactions ID# 0027537 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Debit Acceptor – Canada Region	A Merchant that accepts Visa Debit Category Cards issued by Canadian Issuers. ID# 0025286 Edition: Apr 2020 | Last Updated: Oct 2012
Visa Debit Category – Canada Region	A category of Cards issued by Canadian Issuers that consists of the following: • Debit Cards • Visa Business Debit Cards ID# 0027281 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Debit Category – US Region	A Card category that consists of the following: • Debit Card issued by a US Issuer • Prepaid Card issued by a US Issuer • Card issued by a non-US Issuer

Visa Core Rules and Visa Product and Service Rules

	ID# 0025289　　　　　　　　　　　　　　　　　　**Edition: Apr 2020 | Last Updated: Apr 2020**
Visa Debit Transaction – Canada Region	A transaction using a Visa Debit Category Card. Where a transaction initiated with a Visa Debit Category Card is conducted at a merchant which is not a Visa Debit Acceptor, it will not be a Visa Debit Transaction. Where a transaction initiated with a Visa Debit Category Card is conducted at a merchant where the cardholder selects another payment service, other than Visa Debit, it shall not be a Visa Debit Transaction.
	ID# 0025290　　　　　　　　　　　　　　　　　　**Edition: Apr 2020 | Last Updated: Oct 2012**
Visa Digital Commerce Program (VDCP)	A Visa program (which may include Visa tokenization services) for Acquirers and other approved participants seeking to develop and offer products and services to support Visa digital commerce experiences.
	ID# 0030680　　　　　　　　　　　　　　　　　　**Edition: Apr 2020 | Last Updated: New**
Visa Digital Commerce Program (VDCP) Documentation	A suite of documents that govern participation and implementation requirements for the Visa Digital Commerce Program (VDCP), that comprises all of the following: *Visa Digital Commerce Program Data Privacy and Security Terms and Role Requirements* *Visa Digital Solutions API Reference Guide* *Visa Ready Program for VDCP Digital Terminal Qualification and Solution Approval Process Guide* *Visa Secure Remote Commerce Digital Acceptance Gateway API Reference* *Visa Secure Remote Commerce Digital Acceptance Gateway Implementation Guide* *Visa Secure Remote Commerce SDK Reference* *Visa Secure Remote Commerce Digital Terminal Implementation Guide* *Visa Token Service e-Commerce/Card-on-File Implementation Guide for Token Requestors*
	ID# 0030686　　　　　　　　　　　　　　　　　　**Edition: Apr 2020 | Last Updated: New**
Visa Direct Connect	A direct connection between a Merchant and VisaNet that uses Visa Merchant Direct Exchange or a Visa-approved API-based access

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	method for authorized access for Authorization or Online Financial Transaction processing in the V.I.P. System.
	ID# 0030559 Edition: Apr 2020 | Last Updated: Apr 2018
Visa Drive Card – Europe Region	A Card that is used for the purchase of fuel and vehicle maintenance services and issued as a Visa Business Card, Visa Corporate Card, or Visa Purchasing Card.
	ID# 0029755 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Easy Payment Service (VEPS)	A service that permits qualified Merchants to process small value Transactions in a Card-Present Environment without requiring Cardholder Verification or the issuance of a Transaction Receipt unless requested by the Cardholder.
	ID# 0025697 Edition: Apr 2020 | Last Updated: Oct 2017
Visa Electron Acquirer	A Member that both:
	• Signs a Visa Electron Merchant or disburses currency to a Cardholder using a Visa Electron Card in a Manual Cash Disbursement
	• Directly or indirectly enters the resulting Transaction Receipt into Interchange
	ID# 0025294 Edition: Apr 2020 | Last Updated: Apr 2010
Visa Electron Card	A Card that bears the Visa Brand Mark with the Electron Identifier.
	ID# 0025295 Edition: Apr 2020 | Last Updated: Oct 2013
Visa Electron Merchant	A Merchant that both:
	• Displays the Visa POS graphic with the Electron Identifier or the Visa Brand Mark with the Electron Identifier
	• Has a zero Floor Limit or has a terminal capable of reading and acting upon the Service Code in the Magnetic Stripe or instructions for an Online Authorization Request from a Chip
	ID# 0025299 Edition: Apr 2020 | Last Updated: Oct 2018
Visa Electron Payment Application	A software application contained within a Chip or payment data encoded on a Magnetic Stripe that defines the parameters for processing a Visa Electron Card Transaction and meets the minimum requirements for the Visa Electron Program.

Glossary	
	Glossary
	Visa Core Rules and Visa Product and Service Rules

	ID# 0025300 Edition: Apr 2020 | Last Updated: Oct 2015
Visa Electron Program	A program through which a Member provides payment services to Visa Electron Merchants and Visa Electron Cardholders by acting as a Visa Electron Issuer, Visa Electron Acquirer, or both.
	ID# 0025301 Edition: Apr 2020 | Last Updated: Apr 2010
Visa Employee Benefit Card	A Prepaid Card through which an Issuer enables employers and benefit administrators to provide employees with a Card that allows direct access to benefits such as qualified health care, dependent care, transit, fuel, and meal expenses.
	ID# 0025307 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Europe Authorization Service – Europe Region	The system for Authorization processing of dual-message Transactions, and Authorization and Clearing processing of financial Transactions, operated by Visa in the Europe Region.
	ID# 0029757 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Europe Clearing and Settlement Service (VECSS) – Europe Region	The system and services for Clearing and Settlement, developed, owned, and operated by Visa in the Europe Region.
	ID# 0029758 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Flag Symbol – US Region	A Visa-Owned Mark consisting of the Bands Design with the Visa logo centered in the middle band. A Card must not bear the Visa Flag Symbol.
	ID# 0025316 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Fleet Card	A Visa Commercial Card used for the purchase of fuel and vehicle maintenance services at Merchants classified with one of the following MCCs: 4468, 4582, 5511, 5532, 5533, 5541, 5542, 5599, 7531, 7534, 7535, 7538, 7542, 7549, 7699. In the Europe Region, see Visa Drive Card.
	ID# 0025317 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Fleet Card Application Identifier – Canada Region and CEMEA Region	A Visa Fleet EMV compliant identifier used for Visa Fleet Cards that specifies a unique payment application contained in a compliant Chip Card.
	ID# 0029232 Edition: Apr 2020 | Last Updated: Oct 2015

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

Visa Flexible Spending Account (FSA) – US Region	A Prepaid Card program administered by an employer, in accordance with IRS requirements, that permits employees to set aside pre-tax dollars to pay qualified, out-of-pocket medical expenses not covered by the employer's health care plan. ID# 0025320　　　　Edition: Apr 2020 | Last Updated: Apr 2020
Visa Gift Card	A Prepaid Card designed for consumer gift-giving. ID# 0025321　　　　Edition: Apr 2020 | Last Updated: Apr 2020
Visa Global ATM Network	The network through which an ATM participant provides Cash Disbursement services to Cardholders by acting as an Issuer, an ATM Acquirer, or both. ID# 0025322　　　　Edition: Apr 2020 | Last Updated: Apr 2010
Visa Global Customer Assistance Services	Services, including customer and emergency services, provided by Visa Global Customer Care Services to Cardholders and Issuers. ID# 0024678　　　　Edition: Apr 2020 | Last Updated: Apr 2019
Visa Global Customer Care Services	The 24-hour-a-day, 7-day-a-week centers that provide multilingual emergency assistance services to Cardholders. ID# 0025343　　　　Edition: Apr 2020 | Last Updated: Apr 2019
Visa Higher Priority Payment Application – Europe Region	The Payment Application with the highest priority on a Visa Multichoice Card and a Visa SimplyOne Card. ID# 0029759　　　　Edition: Apr 2020 | Last Updated: Oct 2016
Visa ICS Prescreen Service – US Region	An optional feature of Visa Advanced ID Solutions that allows Members to select data from the Issuers' Clearinghouse Service databases to create a suppression file before mailing solicitations for Cards, non-Visa cards, or other Visa or non-Visa products. ID# 0025000　　　　Edition: Apr 2020 | Last Updated: Oct 2014
Visa Inc.	A Delaware stock corporation. ID# 0025328　　　　Edition: Apr 2020 | Last Updated: Apr 2010
Visa Incentive Card	A Prepaid Card designed to enable a business entity to provide consumer funds in the form of promotional discounts, rebates, or corporate incentives such as bonuses. ID# 0025329　　　　Edition: Apr 2020 | Last Updated: Apr 2020

Glossary	

<div align="center">Glossary</div>

<div align="center">Visa Core Rules and Visa Product and Service Rules</div>

Visa Infinite Business Card	A Visa Business Card that is targeted to small businesses, has the highest value in an Issuer's business product portfolio, and has attributes equal to or exceeding those of a Visa Infinite Card (in the US Region, a Visa Signature Business Card). ID# 0030687 — Edition: Apr 2020 | Last Updated: New
Visa Infinite Card	A product name for a Card that has attributes exceeding those of a Visa Gold Card and Visa Platinum Card. ID# 0025331 — Edition: Apr 2020 | Last Updated: Apr 2020
Visa Infinite Exclusive Privileges	Exclusive privileges made available to Visa Infinite Cardholder through Merchant partnerships. ID# 0025332 — Edition: Apr 2020 | Last Updated: Oct 2015
Visa Infinite Privilege Card – Canada Region	A Card targeted to the high-affluent consumer that has attributes exceeding those of a Visa Infinite Card. ID# 0027720 — Edition: Apr 2020 | Last Updated: Apr 2020
Visa Integrated Circuit Card Specification (VIS)	Chip Card and terminal requirements for Visa Smart Payment programs that serve as companion specifications to the *EMV Integrated Circuit Card Specifications for Payment Systems (EMV)*. ID# 0027328 — Edition: Apr 2020 | Last Updated: Oct 2014
Visa IntelliLink Spend Management	An optional service provided to Members and their Visa Commercial Card clients to access and manage commercial multi-program data, reports, statements, and expense management. ID# 0025614 — Edition: Apr 2020 | Last Updated: Oct 2015
Visa Large Purchase Advantage	A type of Visa Purchasing Card issued to Client Organizations for the purpose of enabling payment for large-ticket purchases in a Commercial Payables environment. ID# 0027089 — Edition: Apr 2020 | Last Updated: Oct 2015
Visa Lower Priority Payment Application – Europe Region	The Payment Application(s) with a lower priority on a Visa Multichoice Card and a Visa SimplyOne Card. ID# 0029760 — Edition: Apr 2020 | Last Updated: Oct 2016
Visa Meetings Card	A Card issued to commercial entities in the public and private sector for commercial purchases associated with business meetings and events.

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	ID# 0025350 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Merchant Direct Exchange	A direct link between a Merchant and VisaNet that uses Visa hardware and commercially available software or other Visa-approved means for authorized access for Authorization or Online Financial Transaction processing in the V.I.P. System.
	ID# 0027068 Edition: Apr 2020 | Last Updated: Apr 2018
Visa Merchant Screening Service	A database of Merchants and Third Party Agents whose contracts with their Acquirers have been terminated for cause, using one of the following listing reason codes: In the Europe Region: 1 – Exceeds objective reporting standards (such as fraud, counterfeit) 2 – Laundering 3 – Excessive Chargebacks/Disputes 4 – Insolvency 5 – Cardholder information misuse 6 – Agreement violation 7 – Card scheme violation 8 – Questionable Merchant In the AP Region: 1 – Deposited fraud transactions 3 – Processed transactions for a third party 4 – Excessive chargebacks and refunds received 5 – Identified in Visa Risk Programs 6 – Acquirer identified fraud activity 7 – Risk of becoming bankrupt, liquidated/insolvent 8 – Violated the merchant agreement 9 – Identified as a Point of Compromise 10 – Involved in fraud in another payment system

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	13 – Illegal Transactions 14 – Suspicious Activity 15 – Bust out Merchant 99 – Other **ID# 0029609** **Edition: Apr 2020	Last Updated: Apr 2019**
Visa Mini Card	A miniaturized version of a Card that must both: • Provide the designated level of utility promised to the Cardholder • Contain the physical elements and data components required to complete a Transaction **ID# 0025355** **Edition: Apr 2020	Last Updated: Apr 2020**
Visa Mobile Payment Application	The payment application that resides in a Mobile Payment Device. **ID# 0026786** **Edition: Apr 2020	Last Updated: Oct 2015**
Visa Mobile Prepaid – AP Region, CEMEA Region, and LAC Region	A mobile-optimized, Visa virtual prepaid product where the Payment Credential is used to access funds stored in an account such as a consumer, business, or Mobile Money Agent's mobile money account. **ID# 0027165** **Edition: Apr 2020	Last Updated: Apr 2020**
Visa Multichoice Card – Europe Region	A Chip Card that includes a combination of two or more Payment Applications on the same account. **ID# 0029761** **Edition: Apr 2020	Last Updated: Oct 2016**
Visa Multinational Program	A Visa program that supports the delivery of Visa commercial solutions to Multinational Companies. **ID# 0026030** **Edition: Apr 2020	Last Updated: Apr 2012**
Visa Multi-Currency Solution	An optional Visa solution that can be added to a consumer Debit Card or Prepaid Card that enables an Issuer to settle with Visa in multiple currencies and to provide its Cardholders the ability to purchase and hold different currencies for transacting internationally. **ID# 0030593** **Edition: Apr 2020	Last Updated: Apr 2020**
Visa Online	A password-protected website that provides Members, VisaNet Processors, and other authorized users with access to Visa information.

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

	ID# 0025360 Edition: Apr 2020 | Last Updated: Oct 2014
Visa Payables Automation	An optional electronic payment solution that enables Issuers to automate their accounts payable processes using Visa Commercial Cards and one of the Visa Commercial Solutions Data and Reporting Tools.
	ID# 0026535 Edition: Apr 2020 | Last Updated: Oct 2012
Visa Payment Application	A software application contained within a Chip or payment data encoded on a Magnetic Stripe that defines the parameters for processing a Visa Transaction and meets the minimum requirements of the Visa Program.
	ID# 0025361 Edition: Apr 2020 | Last Updated: Apr 2010
Visa Payment Controls	An optional Visa service that allows Cardholders to monitor and control Card use by authorizing Issuers to selectively block certain types of Visa Transactions processed through VisaNet, based on the list of available control criteria (for example: MCC, dollar amount, location).
	ID# 0027235 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Payroll	A Prepaid Card that enables employers to offer employees a Card as an alternative to the disbursement of employment wages or salary via a check.
	ID# 0025363 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Platinum	A Card product that has attributes equal to or exceeding those of a Visa Gold Card.
	ID# 0025366 Edition: Apr 2020 | Last Updated: Apr 2010
Visa Platinum Business Card	A Visa Business Card targeted to small businesses that has attributes equal to or exceeding those of a Visa Platinum Card.
	ID# 0030688 Edition: Apr 2020 | Last Updated: New
Visa Premium Corporate Card – LAC Region	A Visa Corporate Card targeted to mid-to-large size companies that is primarily used to pay for senior executives' business travel and entertainment expenses.
	ID# 0027754 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Products	Cards, components, or secure features that relate to Card production,

Glossary

Glossary

Visa Core Rules and Visa Product and Service Rules

	manufacture, personalization, or fulfillment by a Visa-approved manufacturer, Third-Party Personalizer, or Visa-approved fulfillment vendor.
	ID# 0029645 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Program	A program through which a Member provides product- or payment-related services to Cardholders or Merchants by acting as an Issuer, an Acquirer, or both. In the Canada Region: A Visa Program may be an aggregation of individual Card programs.
	ID# 0025377 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Purchasing Card	A Card issued to commercial entities (public and private) that is used for commercial purchases.
	ID# 0025380 Edition: Apr 2020 | Last Updated: Apr 2020
Visa ReadyLink – US Region	A Visa processing service that enables the Authorization and Settlement, through VisaNet, of funds associated with an Issuer-approved load Transaction to a Prepaid Card or to another non-Visa-branded account at a Prepaid Partner.
	ID# 0025384 Edition: Apr 2020 | Last Updated: Apr 2020
Visa Region	Any of the 6 national or multinational geographic areas, as follows: ● Asia-Pacific (AP) Region ● Canada (CAN) Region ● Central and Eastern Europe, Middle East and Africa (CEMEA) Region ● Europe Region ● Latin America and Caribbean (LAC) Region ● United States of America (US) Region
	ID# 0025386 Edition: Apr 2020 | Last Updated: Oct 2016
Visa Resolve Online	An online Visa service for the retrieval and transmission of dispute resolution information and documentation. In the Europe Region: See Electronic Documentation Transfer Method.
	ID# 0025388 Edition: Apr 2020 | Last Updated: Oct 2017

Glossary

Visa Core Rules and Visa Product and Service Rules

Visa Restricted	A classification label assigned to Visa proprietary information (highly sensitive business or technical information) or personal data that requires the highest degree of protection and the strictest standards of diligence and care to prevent unauthorized disclosure or business harm to Visa. Visa Restricted information that contains identifiable Cardholder data or personally identifiable information and is subject to regulatory requirements or industry compliance standards is further classified as "Visa Restricted – Personal Data." ID# 0030035 — Edition: Apr 2020 | Last Updated: Apr 2018
Visa SavingsEdge – US Region	A program designed for small businesses to enable enrolled Cardholders to receive discounts in the form of statement credits for qualifying purchases made at participating Merchants. ID# 0026272 — Edition: Apr 2020 | Last Updated: Oct 2018
Visa Scheme Processor – Europe Region	A Member or a third party that provides Authorization, Clearing, Settlement, or payment-related processing services for Merchants or Members. ID# 0029764 — Edition: Apr 2020 | Last Updated: Oct 2016
Visa Secure	A Visa-approved Authentication Method based on the 3-D Secure Specification. ID# 0030615 — Edition: Apr 2020 | Last Updated: Oct 2019
Visa Settlement Bank	A bank where Visa maintains its Settlement accounts and performs funds transfer for Settlement. ID# 0025391 — Edition: Apr 2020 | Last Updated: Apr 2010
Visa Signature Business – CEMEA Region	A Card that is issued as specified in *Section 4.16, Visa Signature Business* ID# 0029188 — Edition: Apr 2020 | Last Updated: Apr 2020
Visa Signature Business Card – LAC Region	A Visa Business Card that has attributes equal to or exceeding those of a Visa Signature Card and that is targeted to small businesses. ID# 0029980 — Edition: Apr 2020 | Last Updated: Apr 2017
Visa Signature Card	A product name for a Card that has attributes exceeding those of a Visa Gold Card and Visa Platinum Card. ID# 0025394 — Edition: Apr 2020 | Last Updated: Apr 2020

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Visa SimplyOne Card – Europe Region	A Chip Card that includes a combination of two Payment Applications, including duplications of application instances, on two different Payment Credentials. ID# 0029766 — Edition: Apr 2020 | Last Updated: Apr 2020
Visa Smart Payment	EMV-Compliant and VIS-Compliant applications that provide payment service options and controls to Issuers of Chip Cards bearing the Visa Brand Mark or the Visa Brand Mark with the Electron Identifier. ID# 0025397 — Edition: Apr 2020 | Last Updated: Apr 2013
Visa Surcharge Cap – US Region and US Territories	For a Merchant in the US Region or a US Territory, the average Merchant Discount Rate that a Merchant pays to its Acquirer for Credit Card Transactions. The average Merchant Discount Rate is calculated based on Credit Card Transactions conducted by the Merchant for the preceding one or 12 months, at the Merchant's option. ID# 0027538 — Edition: Apr 2020 | Last Updated: Apr 2020
Visa Token Service Active Issuer Participant	An Issuer that has performed the onboarding process with Visa to participate in the Visa Token Service. ID# 0030569 — Edition: Apr 2020 | Last Updated: Oct 2018
Visa Token Service Basic Issuer Participant	An Issuer in a country listed in the *Visa Token Service Basic Issuer Participation Service Guide* that has been enrolled by Visa to participate in the Visa Token Service for Card-Absent Environment Transactions. ID# 0030570 — Edition: Apr 2020 | Last Updated: Oct 2018
Visa Traditional – US Region	A Visa Consumer Credit Card, excluding Visa Signature, Visa Signature Preferred, and Visa Infinite. ID# 0025399 — Edition: Apr 2020 | Last Updated: Oct 2015
Visa Traditional Rewards Card – US Region	A consumer credit product that enables Cardholders, based on their qualifying purchases, to earn units of rewards currency consisting of either: • Points that are redeemable for cash, cash-equivalent rewards (gift certificate, gift card, or statement credit), or any other reward option permitted upon prior approval by Visa • Air miles that are redeemable for air travel ID# 0025400 — Edition: Apr 2020 | Last Updated: Oct 2014

Glossary	

<div align="center">Glossary</div>

<div align="center">Visa Core Rules and Visa Product and Service Rules</div>

Visa Transaction Alerts Service	An optional Visa service that enables Cardholder notification of Transactions occurring on their Cards or accounts in near-real time. ID# 0025728 · Edition: Apr 2020 | Last Updated: Oct 2015
Visa Transaction Information	Any Transaction information or data that is contained in either the Authorization message or Clearing Record. ID# 0025402 · Edition: Apr 2020 | Last Updated: Oct 2016
Visa US Common Debit Application Identifier – US Region and US Territories	An EMV-compliant Application Identifier licensed for use with EMV- and VIS-based applications for the purpose of processing a transaction covered by the Dodd-Frank Act and Federal Reserve Board Regulation II on certain debit products. ID# 0027582 · Edition: Apr 2020 | Last Updated: Oct 2014
Visa US Regulation II Certification Program – US Region and US Territories	A certification program that enables an Issuer in the US Region or a US Territory to certify the status of its consumer debit, commercial debit, and prepaid portfolios in alignment with US Federal Reserve Board Regulation II, 12 CFR Part 235. The program also enables an Issuer in the US Region or a US Territory to notify Visa of its compliance with the final fraud-prevention standards of the US Federal Reserve Board Regulation II, 12 CFR Part 235. ID# 0026999 · Edition: Apr 2020 | Last Updated: Oct 2014
Visa Worldwide Pte. Ltd.	The organization operating the Visa Network in the AP Region. ID# 0025416 · Edition: Apr 2020 | Last Updated: Apr 2010
Visa-Owned Marks	All trademarks and other brand assets (for example: animation, sound, haptic) owned by Visa. ID# 0025216 · Edition: Apr 2020 | Last Updated: Oct 2018
Visa/Plus ATM	An ATM that: • Displays the Visa Brand Mark and the Plus Symbol • May also display the Visa Brand Mark with the Electron Identifier ID# 0025368 · Edition: Apr 2020 | Last Updated: Apr 2010
VisaNet	The systems and services, including the V.I.P. System, Visa Europe Authorization Service, BASE II, and the Visa Europe Clearing and Settlement System, through which Visa delivers online financial

	processing, Authorization, Clearing, and Settlement services to Members, as applicable.
	ID# 0025218 Edition: Apr 2020 | Last Updated: Oct 2016
VisaNet Interchange Center	A Visa facility that operates the VisaNet data processing systems and support networks.
	In the Europe Region: This rule does not apply. Where a Member uses Visa for processing, as specified in *Section 1.1.1.2, Applicability of Processing Rules – Europe Region,* it must refer to *Visa Europe Operating Regulations – Processing*.
	ID# 0025229 Edition: Apr 2020 | Last Updated: Oct 2016
VisaNet Processor	A Member, or Visa-approved non-Member, that is directly connected to VisaNet and that provides Authorization, Clearing, or Settlement services to Merchants and/or Members.
	In the Europe Region: See also Visa Scheme Processor.
	ID# 0025230 Edition: Apr 2020 | Last Updated: Oct 2016
VisaNet Settlement Service	The VisaNet system that provides Settlement reporting and funds transfer services to BASE II and V.I.P. System Clearing Processors.
	ID# 0025232 Edition: Apr 2020 | Last Updated: Oct 2016
Voice Authorization	An Approval Response obtained through interactive communication between an Issuer and an Acquirer, or their VisaNet Processors through telephone or facsimile communications.
	ID# 0025417 Edition: Apr 2020 | Last Updated: Oct 2016
W	
Waiver	A temporary, formal consent granted by Visa that permits a Member or Members to not comply with one or more specific rules in the Visa Rules for a specified period of time.
	ID# 0026498 Edition: Apr 2020 | Last Updated: Oct 2016
Wire Transfer Money Order – US Region	A check or money order purchased by a Cardholder from a Wire Transfer Money Order Merchant.
	ID# 0025434 Edition: Apr 2020 | Last Updated: Oct 2014
Wire Transfer Money Order Merchant – US	A Merchant that sells money orders by electronic funds transfer.

Glossary	
Glossary	
Visa Core Rules and Visa Product and Service Rules	

Region	
	ID# 0025435 Edition: Apr 2020 | Last Updated: Oct 2014
Wire Transfer Money Order Transaction – US Region	A Quasi-Cash Transaction representing the sale of a Wire Transfer Money Order for transfer to a payee (who may or may not be the Cardholder) by electronic funds transfer.
	ID# 0025436 Edition: Apr 2020 | Last Updated: Oct 2014
Workout Period	As a part of the Visa Dispute Monitoring Program (VDMP) and Visa Fraud Monitoring Program (VFMP), a 3-month remediation period during which Visa manages a corrective-action plan between a Merchant and its Acquirer to bring the Merchant's Dispute or Fraud Activity within acceptable levels. The Workout Period is not applicable to any of the following: • High-Brand Risk Merchants, as specified in *Section 10.4.6.1, High-Brand Risk Merchants* • Merchants that exceed the excessive Dispute or Fraud Activity thresholds • Merchants that are escalated to the VDMP high-risk program or the VFMP high-risk program if Visa determines that the Merchant's activities may cause undue harm to the goodwill of the Visa system
	ID# 0025701 Edition: Apr 2020 | Last Updated: Oct 2019
X	
No glossary terms available for X.	ID# 0025513 Edition: Apr 2020 | Last Updated: Apr 2010
Y	
No glossary terms available for Y.	ID# 0025514 Edition: Apr 2020 | Last Updated: Apr 2010
Z	
No glossary terms available for Z.	ID# 0030575 Edition: Apr 2020 | Last Updated: Oct 2018

EXHIBIT D

Terms of Service - Updated on May 3, 2016

Welcome to MySchoolBucks.com. Heartland Payment Systems, Inc. and its affiliates and partners provide this service to you ("you" or "your" means any person using the website or service) subject to the following conditions. If you check the consent box on the registration page or use the MySchoolBucks.com website and service (collectively the "Service"), you accept these terms and conditions. Please read them carefully.

Privacy

Please review our Privacy Policy, which also governs your visit to MySchoolBucks.com, to understand our practices.

Electronic Communications

When you visit MySchoolBucks.com or send emails to us, you are communicating with us electronically. You consent to receive communications from us electronically. We will communicate with you by email or by posting notices on this website. You agree that all agreements, notices, disclosures and other communications that we provide to you electronically satisfy any legal requirement that such communications be in writing.

SMS Communications

When you opt-in to the service, we will send you an SMS message to confirm your signup.

You can cancel the SMS service at any time. Just text "**STOP**" to **58864**. After you send the SMS message "**STOP**" to us, we will send you an SMS message to confirm that you have been unsubscribed. After this, you will no longer receive SMS messages from us. If you want to join again, just sign up as you did the first time and we will start sending SMS messages to you again.

If at any time you forget what keywords are supported, just text "**HELP**" to **58864**. After you send the SMS message "**HELP**" to us, we will respond with instructions on how to use our service as well as how to unsubscribe.

We are able to deliver messages to the following mobile phone carriers:

Major carriers: AT&T, Verizon Wireless, Sprint, T-Mobile, U.S. Cellular, Alltel, Boost Mobile, Nextel, and Virgin Mobile.

Minor carriers: Alaska Communications Systems (ACS), Appalachian Wireless (EKN), Bluegrass Cellular, Cellular One of East Central IL (ECIT), Cellular One of Northeast Pennsylvania, Cincinnati Bell Wireless, Cricket, Coral Wireless (Mobi PCS), COX, Cross, Element Mobile (Flat Wireless), Epic Touch (Elkhart Telephone), GCI, Golden State, Hawkeye (Chat Mobility), Hawkeye (NW Missouri), Illinois Valley Cellular, Inland Cellular, iWireless (Iowa Wireless), Keystone Wireless (Immix Wireless/PC Man), Mosaic (Consolidated or CTC Telecom), Nex-Tech Wireless, NTelos, Panhandle Communications, Pioneer, Plateau (Texas RSA 3 Ltd), Revol, RINA, Simmetry (TMP Corporation), Thumb Cellular, Union Wireless, United Wireless, Viaero Wireless, and West Central (WCC or 5 Star Wireless).

As always, message and data rates may apply for any messages sent to you from us and to us from you. If you have any questions about your text plan or data plan, it is best to contact your wireless provider.

For all questions about the services provided by this short code, you can send an email to support@myschoolbucks.com.

Copyright

All content, titles, graphics, logos, button icons, images and software are the copyrighted material of Heartland Payment Systems, Inc., or its licensors, and you agree not to download (other than page caching) or modify it, or any portion of it. The compilation of all content on this website is the exclusive property of Heartland Payment Systems,

Inc., and is protected by U.S. and international copyright laws. Reproduction, republication or distribution of any material from the website is strictly prohibited, except that you may, for personal and non-commercial use only, make a single hard copy of your transactions for your personal records.

Trademarks

The MySchoolBucks.com name, logo, button icons, child character, and all related logos, products and services described in this website are trademarks or registered trademarks of Heartland Payment Systems, Inc. The MySchoolBucks name and logo are trademarks or registered trademarks of Heartland Payment Systems, Inc. All other trademarks that appear on this website that are not owned by Heartland Payment Systems, Inc., or its affiliates, are the property of their respective owners.

License and Site Access

Heartland Payment Systems, Inc. grants you a limited license to access and make personal use of this Service to pay your child's school for goods and services sold by the school and/or school district (i.e., school meals). You may also be able to use the Service to obtain information about the balance of meal prepayments at your child's school, and to review your child's food purchases at the school cafeteria. You acknowledge and agree that we shall not be held responsible for the accuracy of this information since the content is electronically provided to MySchoolBucks.com from the school or third parties software systems and the accuracy of the content is outside of our control. MySchoolBucks.com shall not be responsible for any loss or damages caused or alleged to have been caused by the use of or reliance on any such content. The Service is intended to be used by adults who can purchase with a credit card. If you are under 18, you may use MySchoolBucks.com only with involvement of a parent or guardian. You are responsible for protecting the confidentiality of your password and should not permit any other person to use your password. You will hold Heartland Payment Systems, Inc. harmless for any activity in your account, including, but not limited to, authorized or unauthorized charges to your credit card or bank information via the Service or disputes between you and the school or school district. Heartland Payment Systems, Inc. reserves the right to refuse service, terminate accounts, or cancel orders according to our discretion.

Payment to Schools

You may make payments to your child's school account by using a credit card. Your credit card provider may have imposed a maximum amount which can be placed on your credit card. Your child's school receives the full payment. Payments are processed promptly for your child's use. However, we make no representations or warranties regarding the amount of time needed to complete processing. A number of factors, such as delays in the banking system, electronic funds transfer systems or school district network, are outside our control and will affect when the funds are received by your child's school. Use of prepayments at your child's school is governed exclusively by your agreement or arrangement with the school or school district, and we are not responsible for the school's handling of your prepayments after the school receives the funds from the Service, including, but not limited to, any failure by a district to record, apply or refund a payment made by you via the Service.

ONE TIME PAYMENTS

You authorize MySchoolBucks to debit the bank account indicated in this web form for the noted amount on today's date. You understand that because this is an electronic transaction, these funds may be withdrawn from your account as soon as the above noted transaction date. You acknowledge that the origination of ACH transactions to your account must comply with the provisions of U.S. law. You will not dispute MySchoolBucks from debiting your checking/savings account, so long as the transaction corresponds to the terms indicated in the web form.

RECURRING PAYMENTS

You authorize MySchoolBucks to debit the bank account indicated in this web form for the noted amount on the schedule indicated. You understand that this authorization will remain in effect until the scheduled end date, or until you cancel the payment, whichever comes first. If the above noted payment falls on a weekend or holiday, you understand that the payment may be executed on the next business day. You understand that because this is an electronic transaction, these funds may be withdrawn from your account each period as soon as the above noted

transaction date. You acknowledge that the origination of the ACH transactions to your account must comply with the provisions of U.S. law. You will not dispute MySchoolBucks recurring billing with your bank so long as the transaction corresponds to the terms indicated in this agreement.

Refunds

If you or your child are not satisfied with any good or service purchased using the Service, you agree to resolve the issue with the child's school or school district. Heartland Payment Systems, Inc. and its affiliates are not responsible for refunds. If you would like a refund of any kind from your child's school or school district, less any program fee, you must contact your child's school. Refund policies may vary from one school district to another.

Program Fee or Membership Fee

Your school district may require a program fee or membership fee for your use of the Service.

If you are required to pay a program fee, you will be notified on a screen prior to completing the payment transaction and any such program fee will be required for each payment you make using the Service.

Links to Third Party Websites

MySchoolBucks.com may contain links to other Internet websites or resources. We neither control nor endorse such other websites, nor have we reviewed or approved any content that appears on such other sites. You acknowledge and agree that we shall not be held responsible for the legality, accuracy, or inappropriate nature of any content, advertising, products, services, or information located on or through any other websites, nor for any loss or damages caused or alleged to have been caused by the use of or reliance on any such content.

LIMITED LIABILITY; DISCLAIMER OF WARRANTY

THE SERVICE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. HEARTLAND PAYMENT SYSTEMS, INC., AND ITS AFFILIATES AND PARTNERS, MAKE NO WARRANTY AND DISCLAIM LIABILITY THAT THE SERVICE WILL BE UNINTERRUPTED, ERROR FREE OR FREE FROM VIRUSES OR OTHER DEFECTS OR HARMFUL COMPONENTS, NOR DO WE MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICE, OR AS TO THE ACCURACY, RELIABILITY OR CONTENT OF ANY INFORMATION PROVIDED THROUGH THE SERVICE. WE MAKE NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, NONINFRINGEMENT, OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. YOU EXPRESSLY AGREE THAT THE USE OF THIS SERVICE IS AT YOUR SOLE RISK.

MYSCHOOLBUCKS IS A CONVENIENT ALTERNATIVE PAYMENT METHODOLOGY BUT IS NOT THE ONLY WAY TO MAKE PAYMENTS TO YOUR SCHOOL. IN THE EVENT MYSCHOOLBUCKS IS NOT AVAILABLE AT ANY TIME FOR ANY REASON YOU ARE ADVISED TO MAKE ALTERNATIVE PAYMENT ARRANGEMENTS. HEARTLAND PAYMENT SYSTEMS, INC. IS NOT RESPONSIBLE FOR THE CONSEQUENCES OF ANY FAILURE BY THE SCHOOL TO RECEIVE ANY PAYMENT.

TO THE FULL EXTENT PERMISSABLE BY APPLICABLE LAW, THIS DISCLAIMER OF LIABILITY APPLIES TO ANY CLAIMS, LOSSES, ACTIONS, DAMAGES OR INJURY RESULTING FROM ANY FAILURE OF PERFORMANCE OF THE SERVICE, ERROR, OMISSION, INACCURACY, INTERRUPTION, DEFECT, DELAY OR INTERRUPTION IN OPERATION OR TRANSMISSION, COMMUNICATION LINE FAILURE, SECURITY BREACH, UNAUTHORIZED ACCESS TO, ALTERATION OF OR USE OF INFORMATION. IN NO EVENT SHALL HEARTLAND PAYMENT SYSTEMS, INC., OR IT AFFIALIATES, BE LIABLE FOR ANY DAMAGES OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE SERVICE, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, INCIDENTAL, PUNITIVE AND CONSEQUENTIAL DAMAGES. CERTAIN STATES DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

Termination

You may terminate this Agreement at any time by providing written notice to us. Heartland Payment Systems, Inc. may immediately terminate this Agreement at any time without notice and for any reason, including, but not limited to, if you engage in any conduct which we, in our sole discretion, consider to be unacceptable, or if you breach this Agreement.

Applicable Law

By visiting MySchoolBucks.com, you agree that the laws of the State of New Jersey will govern these Terms of Use, and any dispute relating to the Service provided herein shall be subject to the jurisdiction of the courts of the State of New Jersey.

Site Policies, Severability

This Agreement and other agreements, policies and any operating rules posted on the Service constitute the entire agreement between you and us with respect to use of the Service, and supersede all previous written or oral agreements between the parties with respect to such subject matter. Heartland Payment Systems, Inc., reserves the right at any time to change, add or delete any aspect or feature of the Service and the terms and conditions thereof, including but not limited to, respective program fees. We will provide notice of any such change by posting a notice to the website or as otherwise required by law. Any use of the Service by you after such notice shall be deemed to constitute acceptance by you of such changes. Any waiver of our rights must be in writing and signed by us. Should any provision of this Agreement be held invalid or unenforceable by any court of competent jurisdiction, the remaining provisions shall remain in full force and effect.

Mobile Apps

Get Social

Quick Links

For Parents

For Schools

Partnerships

For Developers

Mobile Apps

Security

About MySchoolBucks

Our Story

Contact Us

Help

Accessibility

Privacy Policy

Terms of Service

Heartland

A **Global Payments** Company