Mastercard Rules

13 December 2022

BM

Contents

Summary of changes, 13 December 2022

This is a summary of the changes that have occurred since the 6 December 2022 publication of the manual.

Chapter Number	Rule Name	Source or Explanation of Revisions
Chapter 7 Service Providers and Network Enablement Partners	7.1 Service Provider Categories and Descriptions	Updated table
	7.8 Payment Facilitator Obligations	Updated value 1,000,000 to 10,000,000

Summary of changes, 6 December 2022

This is a summary of the changes that have occurred since the previous publication of the manual.

Chapter Number	Rule Name	Source or Explanation of Revisions
Throughout		References to China changed to Mainland China where applicable; references to Macedonia changed to North Macedonia
Applicability of Rules in this Manual	Mastercard Mobile Remote Payment (MMRP) Transactions	AN 6765 Revised Standards for the Decommissioning of Mastercard Mobile
Chapter 1 The License and Participation	1.7.2 Extension of Area of Use Programs	AN 6135 Revised Standards for Extension of Area of Use Programs
	1.2 Mastercard Anti-Money Laundering and Sanctions Requirements 1.2.1 Anti-Money Laundering Requirements 1.2.1.1 Monitoring of Suspicious Activity 1.2.2 Sanctions Requirements	AN 6467 Revised Standards for Anti-Money Laundering and Sanctions Requirements
Chapter 3 Customer Obligations	3.2 Responsibility for Transactions 3.17 BINs	AN 6398 Revised Standards for Service Providers and Customer Asset Disclosure Requirements
	3.13 Privacy and Data Protection 3.13.1 Processing of Personal Data for Purposes of Activity and Digital Activity 3.13.2 Data Subject Notice and Consent 3.13.3 Data Subject Rights 3.13.6 Sub-Processing 3.13.8 Regional Variances and Additions	AN 6854 Revised Standards for Privacy and Data Protection for Mastercard Rules

Chapter Number	Rule Name	Source or Explanation of Revisions
Chapter 4 Use of the Marks	4.4 Signage System 4.4.2 ATM Terminal Signage	AN 6765 Revised Standards for the Decommissioning of Mastercard Mobile
Chapter 5 Acquiring Activity	5.1.2.1 Gambling Merchants	Item 3 has been revised to clarify that the prohibited crediting of winnings or value usable for gambling or gaming refers to the use of a refund transaction.
	5.4.2 Supplying Materials	AN 6426 Revised Standards for QR Enablement in Singapore
	5.8.1 Card Acceptor Business Code (MCC) Information	AN 6298 Revised Standards for Use of Card Acceptor Business Codes 4829 and 6540
	5.8.6 Enablement of QR-based Payments	AN 6646 Revised Standards for Domestic QR Transactions in Argentina
	5.12.5 Existing Mastercard Cardholder Obligations	AN 7031 Revised Standards for Card Acceptor Business Codes
Chapter 6 Issuing Activity	6.1 Card Issuance—General Requirements	AN 6312 Revised Standards to Help Issuers Mitigate Risk from Crypto Transactions with Crypto Secure AN 6640 Revised Standards for Issuer Participation in Safety Net and Prepaid Monitoring in Select Countries in the Europe and Middle East/Africa Regions
	6.1.6 Enablement of QR-based Payments	AN 6426 Revised Standards for QR Enablement in Singapore
Chapter 7 Service Providers and Network Enablement Partners	7.1 Service Provider Categories and Descriptions 7.6.6 Transaction Identification for ISO and PF Transactions 7.8 Payment Facilitator Obligations 7.8.1 Submerchant Agreement 7.8.2 Obligations as Sponsor of Submerchants	AN 6398 Revised Standards for Service Providers and Customer Asset Disclosure Requirements

Chapter Number	Rule Name	Source or Explanation of Revisions
	7.11.4.2 Mastercard Anti-Money Laundering and Sanctions Requirements 7.11.4.3 Variances (renumbered) 7.11.4.4 Failure to Comply with a Standard (renumbered) 7.11.4.5 Testing of Assets (renumbered)	AN 6467 Revised Standards for Anti-Money Laundering and Sanctions Requirements
Chapter 9 Digital Activity	9.2.8 Enablement of QR-based Payments	AN 6646 Revised Standards for Domestic QR Transactions in Argentina
Chapter 11 Asia/Pacific Region	3.13 Data Protection 3.13.8 Regional Variances and Additions 3.13.8.1 Processing of Personal Data for Purposes of Activity and Digital Activity 3.13.8.2 Data Subject Notice and Consent 3.13.8.3 Data Subject Rights 3.13.8.4 Accountability 3.13.8.5 International Data Transfers 3.13.8.6 Sub-Processing 3.13.8.7 Security and Data Protection Audit 3.13.8.8 Data Retention; Deleting Personal Data 3.13.8.9 Personal Data Breaches 3.13.8.10 Liability for China Data Protection Law Violations 3.13.8.11 Applicable Law and Jurisdiction	AN 6854 Revised Standards for Privacy and Data Protection for Mastercard Rules
	5.4.2 Supplying Materials 6.1.6 Enablement of QR-based Payments	AN 6426 Revised Standards for QR Enablement in Singapore

Chapter Number	Rule Name	Source or Explanation of Revisions
	6.1 Card Issuance—General Requirements	AN 6312 Revised Standards to Help Issuers Mitigate Risk from Crypto Transactions with Crypto Secure AN 6640 Revised Standards for Issuer Participation in Safety Net and Prepaid Monitoring in Select Countries in the Europe and Middle East/Africa Regions
Chapter 12 Canada Region	6.1 Card Issuance—General Requirements	AN 6640 Revised Standards for Issuer Participation in Safety Net and Prepaid Monitoring in Select Countries in the Europe and Middle East/Africa Regions
Chapter 13 Europe Region	Definitions European Economic Area (EEA) definition updated to remove Guernsey and Jersey and add Canary Islands SCA Country, SCA Countries definition (Added) 6.1 Card Issuance—General Requirements	AN 2723 Revised Standards for Europe Region PSD2 RTS Compliance for Remote Electronic Transactions

Chapter Number	Rule Name	Source or Explanation of Revisions
	Definitions 3.16 Issuer Reporting Requirement—EEA, Andorra, Serbia, Bosnia and Herzegovina, Gibraltar, and United Kingdom 4.8 Use of Marks on Maestro and Cirrus Cards 4.9 Use of Marks on Mastercard Cards 5.4.3 Provide Information 5.11.1 Honor All Cards 5.11.2 Merchant Acceptance of Mastercard Cards 5.11.5 Discounts or Other Benefits at the Point of Interaction 5.12.1 Discrimination 5.12.2 Charges to Cardholders 6.1 Card Issuance—General Requirements 6.1.4 Tokenization of Accounts 8.4.2 Bilateral Agreement	AN 6903 Revised Standards for Bosnia and Herzegovina

Chapter Number	Rule Name	Source or Explanation of Revisions
	3.13 Privacy and Data Protection 3.13.8 Regional Variances and Additions 3.13.8.6 International Data Transfers 3.13.8.7 Sub-Processing 3.13.8.8 Government Requests for Personal Data 3.13.8.12 Annexes for Processing of Personal Data Annex 1 to Section 3.13.8: Processing of Personal Data Annex 2 to Section 3.13.8: Technical and Organizational Measures to Ensure the Security of Data Annex 3 to Section 3.13.8: Sub-Processing of Personal Data	AN 6854 Revised Standards for Privacy and Data Protection for Mastercard Rules
	6.13.9 Other Issuer Obligations 6.13.10 Rule Additions and Variations for Russia	AN 6298 Revised Standards for Use of Card Acceptor Business Codes 4829 and 6540
	6.1 Card Issuance—General Requirements	6312 Revised Standards to Help Issuers Mitigate Risk from Crypto Transactions with Crypto Secure AN 6640 Revised Standards for Issuer Participation in Safety Net and Prepaid Monitoring in Select Countries in the Europe and Middle East/Africa Regions
	6.1.4 Tokenization of Accounts	AN 6603 Revised Standards for Issuer Card Provisioning into Click to Pay in Select Countries in the Europe Region AN 6970 Revised Standards for Issuer Card Provisioning into Click to Pay in Ireland

Chapter Number	Rule Name	Source or Explanation of Revisions
	3.16 Issuer Reporting Requirement—EEA, Andorra, Serbia, Bosnia and Herzegovina, Gibraltar, and United Kingdom 8.4.2 Bilateral Agreement	AN 7074 Revised Standards for Andorra
Chapter 14 Latin America and the Caribbean Region	6.1 Card Issuance—General Requirements	AN 6312 Revised Standards to Help Issuers Mitigate Risk from Crypto Transactions with Crypto Secure AN 6640 Revised Standards for Issuer Participation in Safety Net and Prepaid Monitoring in Select Countries in the Europe and Middle East/Africa Regions
	5.8.6 Enablement of QR-based Payments 9.2.8 Enablement of QR-based Payments	AN 6646 Revised Standards for Domestic QR Transactions in Argentina
Chapter 15 Middle East/Africa Region	6.1 Card Issuance—General Requirements	AN 6312 Revised Standards to Help Issuers Mitigate Risk from Crypto Transactions with Crypto Secure AN 6640 Revised Standards for Issuer Participation in Safety Net and Prepaid Monitoring in Select Countries in the Europe and Middle East/Africa Regions
Chapter 16 United States Region	6.1 Card Issuance—General Requirements	AN 6640 Revised Standards for Issuer Participation in Safety Net and Prepaid Monitoring in Select Countries in the Europe and Middle East/Africa Regions
Chapter 18 Value-Added Services	18.2 Definitions	Added "sounds, animations, haptics, visual depictions" to Marks definition

Chapter Number	Rule Name	Source or Explanation of Revisions
	18.1 Introduction/Applicability 18.2 Definitions 18.3.1.2 Business Continuity and Disaster Recovery 18.8.1.2 Termination by Mastercard 18.13.7 Force Majeure	AN 6428 Revised Standards for the Value-Added Services Chapter in the Mastercard Rules

Chapter Number	Rule Name	Source or Explanation of Revisions
	18.2 Definitions 18.6.1 Processing of Personal Data for Purposes of Value-Added Service 18.6.2 Data Subject Notice and Consent 18.6.3 Data Subject Rights 18.6.6 Sub-Processing 18.6.7 Returning or Destroying Personal Data 18.6.8 Europe Region Variances and Additions 18.6.8.6 International Data Transfers 18.6.8.7 Sub-Processing 18.6.8.8 Government Requests for Personal Data 18.6.8.12 Annexes for Processing of Personal Data Annex 1 to Section 18.6.8: Processing of Personal Data Annex 2 to Section 18.6.8: Technical and Organizational Measures to Ensure the Security of Data Annex 3 to Section 18.6.8: Sub-Processing of Personal Data 18.6.10 Mainland China Variances and Additions 18.6.10.1 Processing of Personal Data for Purposes of Value-Added Services 18.6.10.2 Data Subject Notice and Consent 18.6.10.3 Data Subject Rights 18.6.10.4 Accountability 18.6.10.5 International Data Transfers	AN 6854 Revised Standards for Privacy and Data Protection for Mastercard Rules

Chapter Number	Rule Name	Source or Explanation of Revisions
	18.6.10.6 Sub-Processing 18.6.10.7 Security 18.6.10.8 Data Retention; Deleting Personal Data 18.6.10.9 Personal Data Breaches 18.6.10.10 Liability for China Data Protection Law Violations 18.6.10.11 Applicable Law and Jurisdiction	
Chapter 19 Mastercard Mobile Rules	Entire chapter is deleted.	AN 6765 Revised Standards for the Decommissioning of Mastercard Mobile
Appendix A Geographic Regions	Asia/Pacific Region	Changed China to Mainland China
	Europe Region	Changed Macedonia to North Macedonia
Appendix B Compliance Zones	Compliance Zones 6.1.6 Enablement of QR-based Payments	AN 6426 Revised Standards for QR Enablement in Singapore
Appendix C Definitions	Corporation Asset	AN 6398 Revised Standards for Service Providers and Customer Asset Disclosure Requirements
	Acceptor Sponsored Merchant Sponsored Merchant Agreement Sponsor, Sponsorship	AN 6475 Revised Standards for International Organization of Standardization Terminology Alignment
	Data Subject Processing of Personal Data	AN 6854 Revised Standards for Privacy and Data Protection for Mastercard Rules
	Marks	Added "animations" to Marks definition.
	Cardholder Verification Method (CVM) Chip-only MPOS Terminal	AN 7008 Revised Standards for Sunsetting of the Quick Payment Service

Mastercard Standards

Mastercard is dedicated to making payments safe, simple and smart. We have a set of standards ("the Standards") in support of this mission that provides our Customers with clear direction as to their responsibilities. The Standards include the information contained in this Mastercard Rules manual and other manuals, along with guides, bulletins and policies that may be updated from time to time.

The Standards enable growth for Mastercard and for our Customers while ensuring integrity and reliability. They are developed under a set of principles that guide us in our actions and provide a framework under which we operate.

Mastercard and its Customers:

Uphold the value of the Mastercard brands as the choice of payment for consumers, businesses and merchants. Consumers, businesses and merchants have multiple payment options to use and to accept. Mastercard and its Customers operate so as to uphold the value of the Mastercard brands so that our products will be adopted and chosen by these end users.

Act with financial integrity and in compliance with the Standards and the law. Operating programs in a manner that is financially sound, in compliance with the Standards and the law helps us manage risk to Mastercard and to our Customers.

Engage in rigorous fraud management practices. Ensuring that transactions are conducted securely is of the utmost importance. Mastercard and its Customers leverage best-in-class technology and business practices in order to make transactions safe.

Manage systems and programs to support interoperability. The ability to process transactions at a global and local level is a key feature of the Mastercard network. Customers manage their systems and programs to enable the seamless acceptance and processing of Mastercard transactions.

Applicability of Rules in this Manual

This manual contains Rules for Activities and Digital Activity.

The below table describes the applicability of the Rules[1] for particular types of Transactions and Payment Transfer Activity (PTA) Transactions. Please note that the term "POS Transaction" refers to a Transaction that occurs at a Merchant location, whether in a Card-present environment at an attended or unattended POS Terminal, or in a Card-not-present environment. In a Card-not-present environment, this may include electronic commerce ("e-commerce"), mail order, phone order, or recurring payment Transactions, Gaming Payment Transactions, and Mainland China Funds Transfer Payment Transactions.

Refer to the *Transaction Processing Rules* manual for brand-specific Rules relating to acceptance in Card-present and Card-not-present environments and the processing of particular Transaction and Payment Transaction types.

Rules relating to...	**Apply to...**
Mastercard POS Transactions	A POS Transaction conducted with a Mastercard Card. A Mainland China domestic POS Transaction conducted with a Mastercard Card (includes a "Debit Mastercard" Card).
Maestro POS Transactions	A POS Transaction conducted with: • A Maestro Card, or • A Mastercard Card issued from a country or territory other than China using a BIN identified by the Corporation as "Debit Mastercard" and routed to the Single Message System.[2]
ATM Transactions	A Transaction conducted with a Mastercard®, Maestro®, or Cirrus® Card at an ATM Terminal and routed to the Interchange System.
Manual Cash Disbursement Transactions	A cash withdrawal Transaction conducted at a Customer financial institution teller with: • A Mastercard Card, or • A Maestro or Cirrus Card at a Bank Branch Terminal and routed to the Interchange System.

[1] If a particular brand or brands is not mentioned in a Rule that applies to Transactions, then the Rule applies to Mastercard, Maestro, and Cirrus.

[2] In Mainland China, the Standards relating to POS Transactions apply to all domestic Transactions.

Rules relating to...	Apply to...
Payment Transactions	A PTA Transaction that transfers funds to an Account. A Payment Transaction is not a credit that reverses a previous purchase. Includes MoneySend™ Payment Transactions, Gaming Payment Transactions and Mainland China Funds Transfer Payment Transactions.
PTA Transactions	A financial transaction in which funds are transferred from an Originating Institution to a Receiving Customer on behalf of Account Holders pursuant to a PTA Program.

Modifying Words and Acronyms

From time to time, the meanings of the above terms are modified by the addition of another word or acronym. For example, a Debit Mastercard POS Transaction means a Transaction resulting from the use of a Debit Mastercard Card at the point of sale (POS). However, for ease of use, not every modifying term is defined. While Mastercard alone interprets and enforces its Rules and other Standards, these *Mastercard Rules* endeavor to use defined terms and other terms and terminology in a plain manner that will be generally understood in the payments industry.

Variations and Additions to the Rules for a Geographic Area

Variations and/or additions ("modifications") to the Rules are applicable in geographic areas, whether a country, a number of countries, a region, or other area.

In the event of a conflict between a Rule and a modification of that Rule, the modification is afforded precedence and is applicable. The Rules set forth in this manual are Standards and Mastercard has the sole right to interpret and enforce the Rules and other Standards.

Chapter 1 The License and Participation

This chapter contains Rules relating to the License and participation in Activity.

1.1 Eligibility to be a Customer

An entity eligible to be a Customer may apply to become a Customer. No entity may participate in Activity until that entity is approved to be a Customer, has executed the applicable Licenses for the proposed Activity in a form acceptable to the Corporation, and has paid all associated fees and other costs.

NOTE: A modification to this Rule appears in the "Digital Activity" chapter.

The following types of entities are eligible to be a Customer.

1.1.1 Principal or Affiliate

A financial institution or other legal entity authorized to engage in financial transactions in accordance with the laws and government regulations of the country (or any subdivision thereof) in which it is organized or principally engaged in business may apply to be a Principal or an Affiliate.

Any such financial institution or other legal entity must also have the requisite right, power, and authority, corporate and otherwise, to be a Customer of this Corporation and to engage in the proposed Activity, and must have submitted business plans acceptable to the Corporation in accordance with the Standards, including without limitation, Rule 2.2.1.

For purposes of this Rule 1.1.1, "financial transactions" means the making of commercial or consumer loans, the extension of credit, the taking of consumer or commercial deposits, the establishment of prepaid accounts and issuance of electronic money or stored value, or the execution of related payment transactions, including effecting such transactions with payment cards or other access devices or methods.

A financial institution applicant must be regulated and supervised by one or more governmental authorities or agencies authorized and empowered to establish or enforce rules regarding financial transactions and the financial condition, activities, and practices of entities engaging in financial transactions. Any other applicant must satisfy such eligibility criteria as the Corporation may adopt from time to time, consistent with the promotion of safe and sound practices, on a regional, country-by-country or other basis. The decision to admit an applicant as a Principal or Affiliate of the Corporation is made at the sole discretion of the Corporation.

1.1.2 Association

Any legal entity that is Controlled by one or more financial institutions eligible and approved to be a Customer as described in Rule 1.1.1 and that proposes to engage in Mastercard Activity on behalf of one or more of those Customers may apply to be an Association.

Any such entity must have the requisite right, power, and authority, corporate and otherwise, to be a Customer of this Corporation, must have submitted business plans acceptable to the Corporation in accordance with the Standards, including without limitation, Rule 2.2.1. The decision to admit an entity as an Association of the Corporation is made at the sole discretion of the Corporation.

1.1.3 Digital Activity Customer

NOTE: A Rule on this subject appears in the "Digital Activity" chapter.

1.1.4 Payment Transfer Activity Customer

An entity that is or is eligible to be a Principal, Affiliate, Association, or other entity that has been approved by the Corporation for Participation in a Payment Transfer Activity (PTA) Program and that satisfies such eligibility criteria as the Corporation may adopt from time to time, consistent with the promotion of safe and sound business practices, may apply to be a PTA Customer. No entity may Participate in a PTA Program as a PTA Customer until that entity is approved to be a PTA Customer, has executed the applicable PTA Agreement for the proposed PTA Program in a form acceptable to the Corporation, and has paid all associated fees and other costs. Prior to commencing each PTA Program, a PTA Customer must enter into a PTA Agreement with the Corporation for each PTA Program.

An entity may be a Principal for Payment Transfer Activity and an Affiliate for another Activity, or vice versa. An entity applying to Participate as a Principal in Payment Transfer Activity(ies) and that is Participating in another Activity as an Affiliate, must have obtained the express written consent of its Sponsor.

The decision to approve an applicant as a PTA Customer (including, admission of such PTA Customer as an Originating Institution and/or Receiving Customer) is at the discretion of the Corporation.

The eligibility criteria for a PTA Customer includes:

1. As applicable, compliance with the *Payment Card Industry Data Security Standard* (PCI DSS) or other standards related to securing and protecting data as specified in the Standards applicable to a particular PTA Program or as mutually agreed in writing by the PTA Customer and the Corporation for such PTA Program;
2. Compliance with all applicable laws and regulations for each jurisdiction in which the PTA Program is proposed to be conducted;
3. Compliance with all applicable PTA Rules and Standards; and
4. Such other criteria as the Corporation deems necessary or appropriate to safeguard the safety and security of the Corporation and Payment Transfer Activity.

1.2 Mastercard Anti-Money Laundering and Sanctions Requirements

As a condition of being granted a License and/or as a condition of an execution of a PTA Agreement by the Corporation, and on an ongoing basis thereafter, each License applicant and each Customer (together, for purposes of this Rule 1.2, "Customers") must demonstrate to the satisfaction of the Corporation ongoing maintenance of comprehensive anti-money laundering ("AML") and sanctions compliance programs (together, for purposes of this Rule 1.2, "Programs") that safeguard the Corporation and the Interchange System from risk associated

with money laundering, terrorist financing, and violation of sanctions. Each Customer must provide and update the Corporation with the Customer's current Anti Money Laundering Compliance contact and a current Sanctions Compliance contact in the My Company Manager application on Mastercard Connect™.

The Programs are subject to periodic examination at the discretion of the Corporation. Such an examination may be by the Corporation or a designee of the Corporation or other person deemed satisfactory by the Corporation. Any such examination is at the Customer's expense. The Corporation must be provided with a complete copy of the examination report and the Customer shall not engage in any conduct or permit any person within the Customer's control to engage in any conduct, agreement, or understanding that would impair the completeness, accuracy, or objectivity of any aspect of the examination or examination report.

A failure to comply with any of the obligations set forth in this Rule may result in:

- The denial of a License and/or denial of execution of a PTA Agreement;
- License and/or PTA Agreement suspension;
- Noncompliance assessments; and/or
- Such other action as the Corporation may deem necessary or appropriate.

Payment Transfer Activity Variation

In addition to Rule 1.2 (including Rule 1.2.1 and Rule 1.2.2), each PTA Customer must comply with any additional AML and sanction requirements set forth in the Standards applicable to each PTA Program in which it is engaged.

1.2.1 Anti-Money Laundering Requirements

Each Customer conducting or proposing to conduct Activity must have a written AML compliance Program with a policy, procedures, and controls in place to safeguard the Corporation and the Interchange System from and against the use of the Interchange System for money laundering and/or terrorist financing. Each Customer's AML compliance Program must be commensurate with its respective AML risk profile and fully implemented in accordance with this Rule and local regulatory requirements.

A Customer's AML compliance Program must address, in a manner satisfactory to the Corporation, all Activity and include, at a minimum, the following:

1. A process to ensure thorough client identification and due diligence;
2. Sufficient controls, resources, and monitoring systems for the prompt detection and reporting of suspicious activity, including the requirements set forth in Rule 1.2.1.1;
3. Compliance with all regulatory record-keeping and reporting requirements;
4. Risk assessment processes designed to identify and apply appropriate risk management controls;
5. A training program for all personnel whose duties require knowledge of the AML compliance Program and requirements; and
6. An audit process to periodically test controls.

1.2.1.1 Monitoring of Suspicious Activity

To comply with item 2, of Rule 1.2.1, suspicious activity monitoring must be commensurate with the level of risk presented by the Customer's Cardholder and/or Merchant portfolios, Service Providers, and other agents and third parties acting on behalf of the Customer. The Customer is responsible for ensuring that the Customer's suspicious activity monitoring is capable of identifying suspicious activity as it occurs and/or trends over time.

Detection of Suspicious Activity

The Customer must implement, as applicable, the following AML typologies at a minimum as a part of its suspicious activity monitoring, based on the Customer's assessment of the money laundering risk of its Activity and the Customer's risk tolerance:

- Monitoring Cross-Border Transaction Activity and adjusting applicable controls for geographies that the Customer considers higher risk;
- Cardholder or Merchant Transaction monitoring based on the Customer's risk rating of such Cardholder or Merchant;
- Identifying and monitoring MCCs and Transaction types that the Customer considers at a higher risk for money laundering, including identifying and monitoring any Transactions that can facilitate movement of funds, such as fiat from cryptocurrency exchanges, funds transfers, funding of financial instruments or accounts, and cash back, cash out activity;
- Identifying and monitoring the Customer's use of products related to Activity that that Customer considers at a higher risk for money laundering and/or terrorist financing;
- Changes in Activity over time, including out of pattern Activity, increases in Transaction volumes and/or counts, or increasing frequency of Transactions; and
- And any other AML typologies applicable to the Customers business model and risk profile.

Detection of Suspicious ATM Activity

The Customer must monitor ATM Activity as a part of its suspicious activity monitoring, and must implement, as applicable, the following AML typologies at a minimum as a part of its suspicious activity monitoring, based on the Customer's assessment of the money laundering risk of its ATM Activity and tolerance:

- Out-of-pattern ATM withdrawal Transaction volume and/or velocity at an individual ATM or groups of ATMs;
- Sequential or consecutive high Transaction volumes of ATM withdrawals at the same ATM(s) by multiple Cards from the same Issuer;
- Significantly high Transaction volumes of repetitive ATM withdrawals over time;
- Excessive ATM Transaction withdrawals at maximum ATM Transaction limits in a short period of time; and
- Out-of-pattern, excessive or high volumes of ATM deposits.

In addition, the Acquirer of any ATM Owners or Service Providers who process ATM Transactions are obligated to monitor ATM Activity regardless of the monitoring obligation of the Issuer.

Reporting of Suspicious Activity

The Customer must comply with the Customer's local law and regulation requirements to report suspicious Transaction activity involving Cardholders, Merchants, and ATMs and take all such other action as required by Applicable Law related to such activity.

1.2.2 Sanctions Requirements

Each Customer, regardless of where situated, must ensure that Activity is in compliance with the sanctions laws and regulations enacted by United States sanctions authorities (including the United States Office of Foreign Assets Control ["OFAC"] and the United States Department of State), as well as all applicable local sanctions regulations where the Activity is taking place.

A Customer is prohibited from engaging in Activity with any person, including any legal entity or government, or in any geography in contravention of any regulation or other requirement promulgated by the United States sanctions authorities, as well as any applicable local sanctions authority.

Each Customer engaging in or proposing to engage in Activity must have a written sanctions compliance Program that includes a policy, procedures, and controls. The sanctions compliance Program must address, to the satisfaction of the Corporation, all Activity and include, at a minimum, the following:

Sanctions List Screening

1. (i) An Issuer must screen its Cardholders, Service Providers, and other representatives and agents (including, but not limited to, a program manager); (ii) an Originating Institution must screen the Originating Account Holders, the Receiving Account Holders, and entities transferring PTA Transaction funds directly to the Receiving Account Holders, Service Providers, and other representatives and agents (including, but not limited to, a program manager); and (iii) a Receiving Customer must screen the Receiving Account Holders, Service Providers, and other representatives and agents (including, but not limited to, a program manager), in each case at the time of onboarding and on an ongoing basis, against applicable sanctions lists, including, but not limited to, OFAC sanctions lists (such as, the Specially Designated Nationals and Blocked Persons List [the "SDN List"]).
2. An Acquirer must screen its Merchants and Service Providers and other representatives and agents (including, but not limited to, a Third Party Processor [TPP]) at the time of onboarding, and on an ongoing basis, against applicable sanctions lists, including, but not limited to, OFAC sanctions lists (such as, the SDN List).

Prohibited Activity

1. No Activity may be conducted in a geography (country or region) that is the subject of applicable sanctions, including those identified by OFAC.
2. No Activity may be conducted with a person, entity, or government on the OFAC sanctions lists (such as, the SDN List) and other locally applicable sanctions lists.

A Customer must immediately cease any Activity with a person, entity, or government identified as listed on any of the OFAC sanctions lists or locally applicable sanctions lists.

NOTE: Activity with an entity listed on OFAC's Sectoral Sanctions Identifications List ("SSI List") may only be conducted in compliance with the limitations or conditions established by OFAC for that program.

1.3 Satisfaction of Minimum Financial Requirements

Each Customer at all times must satisfy the minimum financial requirements established by the Corporation from time to time.

The Corporation, in its discretion, may establish different or additional financial requirements for (i) a category of financial institutions, organizations, or corporations or other entities that are eligible to become a Customer, or (ii) an individual Customer or prospective Customer in the manner set forth in the Standards should the Corporation determine that different or additional requirements are reasonably appropriate to evidence the financial integrity of a type of Customer or an individual Customer or prospective Customer.

Such requirements may include both objective standards, such as the measurement of capital adequacy, and subjective standards, such as evaluating key management experience and ability, the area in which the Customer engages in business, and the manner in which such business is conducted.

1.4 Special Conditions of Participation, License or Activity

The Corporation may condition Participation, the grant of any License, or the conduct of Activity on compliance by the Customer with special conditions, such as the establishment of escrow arrangements, the delivery of letters of credit, or other arrangements that the Corporation deems necessary or appropriate to maintain the integrity of Mastercard and/or the Interchange System, including but not limited to conditions imposed pursuant to Mastercard Anti-Money Laundering and Sanctions Requirements.

The Corporation has the right at any time to require that a Customer enter into a security arrangement with the Corporation. If a Customer does not enter into a security arrangement with the Corporation that is satisfactory to the Corporation, the Corporation has the right at any time to collect from the Customer, in addition to any amount otherwise due and payable by the Customer to the Corporation or to other Customers, such additional amount from the Customer as collateral as the Corporation deems appropriate. The Corporation has the right to collect any such additional amount by any means available to the Corporation including by way of example and not limitation:

1. By taking any funds deposited by any persons from any account that the Corporation is authorized to draw upon for any purpose.
2. By taking any funds due to such Customer from other Customers.
3. By taking any funds being paid by such Customer to other Customers.

In each case in which the Corporation takes any such collateral, the Corporation has the right to take ownership of all or any part of such collateral (such as by placing funds taken in an account

in the Corporation's name as a secured party) and to apply such collateral as payment toward any obligation of the Customer in accordance with the Standards.

Each Customer hereby appoints and authorizes the Corporation to act as the Customer's attorney and agent for any and all purposes in connection with the filing, recording, or other perfecting of the Corporation's rights under the Standards. This Rule constitutes a security agreement between each Customer and the Corporation, and vests in the Corporation a security interest in any collateral collected as provided in these Standards, granted contemporaneously in exchange and as a condition for the continuation of the Customer's Participation and Licenses.

1.5 Interim Participation

Pending approval of an application to be a Customer, the Corporation may authorize the applicant to participate in Activity on an interim basis as if the applicant were a Customer.

As a condition of such interim authorization, the applicant must agree, and by commencement of any Activity the applicant is deemed to have agreed, to comply during this interim period (and thereafter as applicable) with the Standards and to discontinue immediately any use of the Marks and Activity if the application to be a Customer is declined.

All damages, losses, costs, and liabilities arising directly or indirectly, or consequentially, from or related to any interim participation in Activity by the applicant and from the disapproval of the application to be a Customer is solely at the applicant's risk and expense, and this Corporation has no responsibility for any such damages, losses, costs, or liabilities.

1.6 The License

Each Customer agrees, and by use of any one or more of the Marks agrees, to comply with all provisions of the License pertaining to use of the Marks and with the Standards of this Corporation as may be in effect from time to time.

In the event of an inconsistency between a Standard and a provision in a License, the Standard prevails and the License is deemed to be amended so as to be consistent with the Standard. Each Customer must assist the Corporation in recording any License granted to the Customer if required in the country in which the Customer is Licensed or otherwise upon request of the Corporation.

NOTE: Rules on this subject appear in the "Europe Region" chapter.

1.6.1 SEPA Licensing Program—Europe Region Only

NOTE: Rules on this subject appear in the "Europe Region" chapter.

1.7 Area of Use of the License

Except as otherwise provided in the Standards, each Customer may use a Mark and conduct Activity solely in the Area of Use in which the Customer has been granted a License.

If the License does not specify an Area of Use, the License is deemed to authorize the Customer to use the Mark and conduct Activity only in the country or countries the Corporation determines to be the Customer's Area of Use.

A License that the Corporation deems to be inconsistent with this Rule is deemed amended effective as of the date of the grant of the License so as to be consistent with this Rule.

Except as otherwise provided in the Standards, the ICA number and BIN/IIN or BIN range, as applicable, used to conduct issuing and/or acquiring Activity must reflect the country, from among those in the Customer's Area of Use, (i) where Cards are issued and/or Merchants, ATM Terminals, or Bank Branch Terminals effecting acquired Transactions are located, or (ii) in the case of Payment Transfer Activity, where PTA Accounts are held and/or where, if applicable, Merchants effecting PTA Transactions are located.

NOTE: Modifications to this Rule appear in the "Europe Region" and "Middle East/Africa Region" chapters.

1.7.1 Extending the Area of Use

A Customer must apply to the Corporation for permission to extend the Area of Use of a License.

Such application must be made in the form and include all information then required by the Corporation. If the application is approved, the Corporation will amend the License to reflect the change in the Area of Use.

NOTE: Modifications to this Rule appear in the "Europe Region" and "Middle East/Africa Region" chapters.

1.7.2 Extension of Area of Use Programs

Notwithstanding Rule 1.7, a Customer is not required to apply to extend the Area of Use of a License to conduct any of the following Activities, subject to (a) the Corporation's right to prohibit or restrict or condition any such Activity and (b) compliance by the Customer with Standards, laws and regulations applicable to any such Activity:

1. Issue or distribute Mastercard, Maestro, or Cirrus Cards outside of the Customer's Area of Use, other than in the Russian Federation, provided that:
   a. The Cards are issued or distributed only for one of the following purposes pursuant to a prepaid Card Program that is limited in time and/or related to distress issuance or distribution (excluding payroll and incentive Cards):
      – Secondary Cardholder when the primary Cardholder is located in the Customer's Area of Use;

- Distressed passengers;
- Emergency assistance;
- Humanitarian aid; or
- Non-recurring limited-use disbursements; or

b. As otherwise approved by the Corporation.

2. Issue or distribute Mastercard, Maestro, or Cirrus Cards to citizens of any country within the Customer's Area of Use, wherever such citizens reside.
3. Issue or distribute Mastercard commercial Cards, including but not limited to Mastercard Corporate Card® Cards, to employees of an entity on whose behalf the Cards are issued, wherever such employees reside, provided that the entity is multinational, having a presence and conducting regular business in more than one country, including at least one country in the Customer's Area of Use.
4. Issue or distribute Mastercard payroll or incentive Cards, including but not limited to debit and prepaid Cards, to employees and Independent Contractors of an entity on whose behalf the Cards are issued, other than the Russian Federation, provided that:
   a. The entity is multinational, having a presence and conducting regular business in more than one country, including at least one country in the Customer's Area of Use;
   b. The gross dollar volume (GDV) within a country in a calendar year from the Customer's and its Sponsored Affiliates' total cross-border issuance for all payroll and incentive Card Programs for all entities served in that country does not exceed one percent of that country's Mastercard GDV in the prior calendar year;
   c. If the Customer has a License to issue Cards in a particular country (Country A) but wishes to issue Cards into Country A from another country in which the Customer is also licensed (Country B), the Customer's and its Sponsored Affiliates' total cross-border issuance from Country B into Country A in a calendar year may not exceed:
      - 10 percent of that Customer's and its Sponsored Affiliates' total domestic Mastercard GDV in Country A in the prior calendar year, or
      - If greater than the 10 percent described herein, the amount allowed under the one percent threshold described above; and
   d. The Customer performed full know your customer (KYC) due diligence, identification verification and sanctions screening (against U.S. OFAC and other relevant lists) on each Independent Contractor prior to any such Card issuance or distribution, including as required by Rule 1.2.

   For purposes of this Rule, "Independent Contractor" means a natural person that directly performs work or provides services either for (i) an entity through an agreement as a non-employee; or (ii) third parties introduced to such natural person as part of services provided by such multinational entity to such natural person through an agreement as a non-employee (and for the avoidance of doubt, services include the remittance of payments from such third parties to such natural person), and in each case, where such relationship does not constitute an employment relationship under applicable law or regulation.
5. Issue or distribute single-use Virtual Accounts outside of the Customer's Area of Use to travel agents, other than travel agents located in the Russian Federation, provided that such Virtual Accounts are used to purchase travel services pursuant to the Mastercard Enterprise Solution Wholesale Travel Program;

6. Acquire Mastercard or Maestro airline Transactions from a Merchant located in a country, other than the Russian Federation, that is outside of the Customer's Area of Use, subject to satisfying all of the following requirements:
   a. The airline has a meaningful presence in at least one country, within the Area of Use; and
   b. The Customer identifies the airline Transactions with an ICA and BIN/IIN that reflects either the country, or a country within the same Region as the country, in which the airline ticket office is located; and
   c. The Customer authorizes, clears, and settles each Domestic Transaction in a manner that does not significantly disadvantage an Issuer in the same country in the judgment of the Corporation.
7. Originate MoneySend Payment Transactions as set forth in "Extension of Area of Use Programs" in the *Mastercard MoneySend and Funding Transaction Program Standards*.

The following Standards apply to all of the extension of Area of Use programs described in this Rule, except paragraph 7 as set forth above:

- At least 14 calendar days before a Customer proposes to conduct Activity under any of the extension of Area of Use programs described in this Rule, the Customer must submit a completed certification of extension of Area of Use program form (Form 1336) (the "Certification") to the Corporation by sending an email message to certification@mastercard.com. By submitting the completed form, the Customer certifies that (a) the Activity is in compliance with one or more of the extension of Area of Use programs described in this Rule; and (b) the Customer has conducted extensive due diligence to ensure that the Activity will not violate Mastercard Standards or any local laws or regulations of the country(ies) in which the Activity will be conducted. This Certification is required for Activity conducted pursuant to this Rule. Each Certification is subject to the Corporation's right to prohibit or restrict or condition any such Activity.
- A Customer conducting Activity in accordance with an Area of Use program described under any of paragraph 1 through 5 must use a dedicated BIN or BIN range for such Area of Use program.
- For the avoidance of doubt, the Standards in Rule 1.7.4 take precedence for a Card issued directly or indirectly to residents of India.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region", and "Europe Region", and "Middle East/Africa Region" chapters.

1.7.3 Central Acquiring—Europe Region Only

NOTE: Rules on this subject appear in the "Europe Region" chapter.

1.7.4 Transfer of Cards to India Residents is Prohibited without a License

An Issuer that reasonably believes that its Cardholders will distribute, transfer, or in any way provide Cards issued by the Issuer to residents of India must become Licensed in India and receive written authorization from the Reserve Bank of India.

Unless the Issuer is Licensed in India and has written authorization from the Reserve Bank of India, an Issuer that issues Cards to Cardholders that reside outside of India must communicate to those Cardholders in the terms and conditions of the cardholder agreement that such Cards must not be distributed, transferred, or in any way provided to residents of India.

1.8 The Digital Activity Agreement

NOTE: A Rule on this subject appears in the "Digital Activity" chapter.

1.9 Participation in Activity(ies) and Digital Activity

Each Customer may participate only in Activity as set forth in its License or Licenses.

NOTE: Modifications to this Rule appear in the "Digital Activity" and "United States Region" chapters.

Payment Transfer Activity Variation

The Rule on this subject, as it applies to Payment Transfer Activity, is revised and restated as follows.

Each PTA Customer may Participate only in such PTA Program as is set forth in its License(s) and/or PTA Agreement(s) with the Corporation or as otherwise documented in writing by the Corporation.

1.9.1 Changing Customer Status

In the event that an Affiliate wishes to become a Principal or a Principal wishes to become an Affiliate, the Customer must notify the Corporation and submit such information as the Corporation deems necessary.

It is within the Corporation's discretion whether to grant the requested change in Customer status.

1.9.2 Participation and License, Digital Activity Agreement or PTA Agreement Not Transferable

A Customer must not transfer or assign its Participation or any License or Digital Activity Agreement, whether by sale, consolidation, merger, operation of law, or otherwise, without the written consent of the Corporation.

However, in the event that the Cards issued by, the Ownership of, or any Activity or Digital Activity of a Customer are acquired by any person, whether by sale, consolidation, merger,

operation of law or otherwise, the obligations, but not the rights, of such Customer shall transfer to the person acquiring such Customer.

1.9.3 Right to Sponsor Affiliates

Each Principal and Association has the right to Sponsor as an Affiliate any eligible entity which conducts or proposes to conduct Activity within the Principal's or Association's Area of Use.

1.9.4 Change in Sponsorship of an Affiliate

Each Principal or Association must advise the Corporation promptly if an Affiliate ceases to be Sponsored by the Principal or Association or has a transfer of Ownership or Control.

Refer to Rule 1.13.4, paragraph 9, regarding the obligation of each Principal and Association to accept Transactions arising from Cards issued by formerly Sponsored Affiliates.

1.9.5 Customer Name Change

The Corporation must receive written notice at least 30 days before the effective date of any proposed Customer name change.

A Customer that proposes to change its name must promptly undertake necessary or appropriate action to ensure that its Licenses and Activities disclose the Customer's updated name.

1.9.6 The Sponsored Digital Activity Entity

NOTE: A Rule on this subject appears in the "Digital Activity" chapter.

1.10 Participation in Competing Networks

A Customer may take part, as either an issuer or an acquirer or both, in any ATM network in addition to the Mastercard® ATM Network that is not a Competing ATM Network.

Notwithstanding the foregoing, Customers in the countries listed in Rule 1.10.3 may participate in a Competing ATM Network, but only in the manner and to the extent expressly set forth in the Standards.

A Customer may offer its Cardholders any electronic funds transfer (EFT) services (whether provided by the Mastercard® ATM Network or not), charge its Cardholders such fees, if any, as it chooses, arrange with any Customer or non-Customer for mutual access to ATMs by the Cardholders or cardholders of each, respectively, process and settle any ATM transactions without using the Interchange System, locate its ATMs wherever it chooses, and otherwise conduct its EFT business in the manner it chooses.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region" chapter.

1.10.1 Protection of the Corporation

If a Customer permits cardholders of an entity that is not a Customer to have access to its or its Customer's ATM Terminals, such entity has no participation rights in the Mastercard® ATM Network, and has no right of access to the ATM Terminals of other Customers.

If a Customer takes part in an ATM network other than the Mastercard® ATM Network, it must do so in a manner that is consistent with all applicable provisions of the Standards. It must not, because of such participation, discriminate against the Mastercard® ATM Network, any Customer or its Cardholders, or otherwise fail to comply with the Standards.

1.10.2 Participation Restrictions

A Customer that participates in the Mastercard® ATM Network as an Issuer or Acquirer may not simultaneously participate in a Competing ATM Network except as provided in Rule 1.10.3, specifically:

1. A Card or Portfolio of Cards may not participate in a Competing ATM Network; and
2. A card that provides access to a Competing ATM Network may not be a Card.

For purposes of this Rule, to participate in a Competing ATM Network as a card issuer means to issue cards, pursuant to the rules and regulations of that system, for the purpose of providing access to accounts of the issuer in accordance with such rules and regulations.

Notwithstanding this Rule, a Customer that maintains deposit accounts for individuals on behalf of one or more non-Customers may:

1. Issue to such individuals Cards bearing the name or trade name of such non-Customers that provide access to such individuals' accounts through such Competing ATM Networks; and
2. Authorize Transactions from such systems on behalf of such individuals; provided that:
   a. Any non-Customer whose name appears on such Cards is ineligible to obtain a License from the Corporation for a reason other than its current in another Competing ATM Network,
   b. The name of the Customer does not appear anywhere on such Cards; and
   c. The aggregate of all such Cards issued by the Customer does not exceed ten percent (10 percent) of the total Cards issued by such Customer.

1.10.3 Exceptions to the Participation Restrictions

In the following countries or territories, a Customer that acquires transactions of a Competing ATM Network at its ATMs is not rendered ineligible to be a Customer.

Albania	Andorra	Armenia
Australia	Austria	Azerbaijan
Bahrain	Belarus	Belgium
Bolivia	Bosnia and Herzegovina	Bulgaria

Canada	Caribbean Territory (all countries)	Chile
Cyprus	Croatia	Czech Republic
Denmark	Ecuador	Egypt
Estonia	Fiji	Finland
France	Georgia	Germany
Gibraltar	Greece	Guam
Guernsey	Hong Kong SAR	Hungary
Iceland	India	Indonesia
Ireland	Israel	Italy
Japan	Jersey	Kazakhstan
Korea, Republic of	Kuwait	Kyrgyzstan
Latvia	Liechtenstein	Lithuania
Luxembourg	Mexico	Malaysia
Malta	Moldova	Monaco
Morocco	New Zealand	Montenegro
Netherlands	North Macedonia	Norway
Oman	Paraguay	Peru
Philippines	Poland	Portugal
Russian Federation	Romania	San Marino
Saudi Arabia	Serbia	Singapore
Slovak Republic	Slovenia	South Africa
Spain	Sri Lanka	Sweden
Switzerland	Taiwan	Tajikistan
Thailand	Tunisia	Turkey
Turkmenistan	Ukraine	United Arab Emirates
United Kingdom	United States	United States territories
Uzbekistan	Vatican City State	Venezuela

Vietnam	Zimbabwe

In the following countries or territories, a Customer that participates in a Competing ATM Network as a credit card issuer is not rendered ineligible to be a Customer.

1. Hong Kong SAR
2. Mexico
3. The Philippines
4. Singapore
5. Thailand
6. Venezuela
7. Any country in the Europe Region if authorized by the Corporation

1.11 Portfolio Sale, Transfer, or Withdrawal

The Corporation must receive written notice at least 30 days before the effective date of any proposed transfer or assignment of a Mastercard Portfolio.

A Customer must promptly provide the Corporation any information requested by the Corporation relating to such an event or proposed event. If such transfer or assignment will result in a change of Control of the Customer or the Customer's issuing Program, acquiring Program, or both, then Rule 1.12 shall apply.

A Principal must not withdraw a Maestro or Cirrus Portfolio from participation in the Interchange System except upon fulfillment of the following conditions:

1. The Principal must provide the Corporation with at least six months prior written notice of its intent to withdraw a Portfolio. If confidential negotiations surrounding a Portfolio sale would render six months' notice unduly disruptive, the Corporation may accept a shorter time at its discretion.
2. The Principal must certify in writing to the Corporation that as of the date of withdrawal, no Cards will be in circulation, unless the Corporation has approved a plan for the phased withdrawal of the Portfolio. Any phased withdrawal must not exceed the lesser of one full re-issuance cycle or two years. Any withdrawal plan must guarantee that Cards still in circulation will continue to provide access to Accounts through the Corporation.
3. If there is a new owner of the Portfolio, such owner must be a Customer of the Corporation. Alternatively, if the new owner is not eligible to be Licensed, then it must enter into an agreement with the Corporation to be bound by all Rules applicable to the Portfolio during its withdrawal period.

Payment Transfer Activity Variation

The Rule on this subject, as it applies to Payment Transfer Activity, is revised and restated as follows.

The Corporation must receive written notice at least 30 days before the effective date of any PTA Customer's proposed transfer or assignment of its obligations under the Standards applicable to its Participation in Payment Transfer Activity. A Customer must promptly provide the Corporation any information requested by the Corporation relating to such an event or proposed event. If such transfer or assignment will result in a change of Control of the Customer, then Rule 1.12 shall apply.

1.12 Change of Control of Customer or Portfolio

The Corporation must receive written notice at least 30 days before the effective date of any proposed change of Control of a Customer.

A Customer must promptly provide the Corporation any information requested by the Corporation relating to such an event or proposed event and the Corporation may:

1. Suspend or impose conditions on any Licenses granted to the Customer, any Digital Activity Agreements or any PTA Agreements with the Customer.
2. Amend rights, obligations, or both of a Customer.
3. Terminate the Licenses, Digital Activity Agreements, or PTA Agreements or all of any Customer that:
   a. Transfers or attempts to transfer Control of the Customer to an entity that is not a Customer; or
   b. Merges into or is consolidated with an entity that is not a Customer; or
   c. Sells all or substantially all of its assets; or
   d. Sells all or substantially all of its Issuer or Acquirer Portfolios or PTA Account Portfolios; or
   e. Experiences a change in Control or Ownership.

NOTE: Modifications to this Rule appear in the "United States Region" chapter.

1.13 Termination

The Participation or Licenses or Digital Activity Agreements or PTA Agreements of a Customer may terminate in either of two ways: voluntary termination, or termination by the Corporation.

1.13.1 Voluntary Termination

A Customer may voluntarily terminate its Participation and/or Licenses and/or Digital Activity Agreements and/or PTA Agreements by providing written notice and submitting documentation as then required by the Corporation. The notice must fix a date on which the termination will be effective as follows.

Written notice to the Corporation provided by or with respect to a...	Regarding termination of its...	Must be received in advance of the termination effective date, by at least...
Principal	Mastercard License	30 days
Association	Mastercard License	30 days
Principal	Maestro License	One year
Principal	Cirrus License	One year
Affiliate	Mastercard License	30 days
Affiliate	Maestro License	Six months
Affiliate	Cirrus License	Six months
Digital Activity Customer	Digital Activity Agreement	60 days
PTA Customer	PTA Agreement and/or Payment Transfer Activity License	As set forth in the Standards

When all Licenses, Digital Activity Agreements, and PTA Agreements are terminated, the Participation of a Customer also terminates.

1.13.2 Termination by the Corporation

Notwithstanding anything to the contrary set forth in a License or Digital Activity Agreement, the Corporation, at its sole discretion, may terminate a Customer's Participation effective immediately and without prior notice, if:

1. The Customer suspends payments within the meaning of Article IV of the Uniform Commercial Code in effect at the time in the State of Delaware, regardless of whether, in fact, the Customer is subject to the provisions thereof; or
2. The Customer takes the required action by vote of its directors, stockholders, members, or other persons with the legal power to do so, or otherwise acts, to cease operations and to wind up the business of the Customer, such termination to be effective upon the date of the vote or other action; or
3. The Customer fails or refuses to make payments in the ordinary course of business or becomes insolvent, makes an assignment for the benefit of creditors, or seeks the protection, by the filing of a petition or otherwise, of any bankruptcy or similar statute governing creditors' rights generally; or
4. The government or the governmental regulatory authority having jurisdiction over the Customer serves a notice of intention to suspend or revoke, or suspends or revokes, the operations or the charter of the Customer; or
5. A liquidating agent, conservator, or receiver is appointed for the Customer, or the Customer is placed in liquidation by any appropriate governmental, regulatory, or judicial authority; or
6. The Customer's right to engage in Activity or Digital Activity, as the case may be, is suspended by the Corporation due to the Customer's failure to comply with the

Corporation's Anti-Money Laundering and Sanctions Requirements in connection with its Program or to comply with applicable law or regulation, and such suspension continues for 26 consecutive weeks; or

7. The Customer fails to engage in Activity for 26 consecutive weeks; or
8. The Customer is no longer Licensed to use any of the Marks; or
9. The Customer (i) directly or indirectly engages in or facilitates any action or activity that is illegal, or that, in the good faith opinion of the Corporation, and whether or not addressed elsewhere in the Standards, has damaged or threatens to damage the goodwill or reputation of the Corporation or of any of its Marks; or (ii) makes or continues an association with a person or entity which association, in the good faith opinion of the Corporation, has damaged or threatens to damage the goodwill or reputation of the Corporation or of any of its Marks; or
10. The Customer (i) provides to the Corporation inaccurate material information or fails to disclose responsive material information in or in connection with its application for a License; or (ii) at any other time, in connection with its Participation or Activity fails to timely provide to the Corporation information requested by the Corporation and that the Customer is required to provide pursuant to the terms of the License or the Standards; or
11. The Customer fails at any time to satisfy any of the Customer eligibility criteria set forth in the Standards, or with respect to a Digital Activity Customer, all certifications granted by the Corporation in connection with the Digital Activity Customer's conduct of Digital Activity have been suspended or revoked; or
12. The Customer materially fails to operate at a scale or volume of operations consistent with the business plan approved by the Corporation in connection with the Customer's application to be a Customer or application for a License, or both, as the case may be, as required by Rule 2.2.1; or
13. The Corporation has reason to believe that the Customer is, or is a front for, or is assisting in the concealment of, a person or entity that engages in, attempts or threatens to engage in, or facilitates terrorist activity, narcotics trafficking, trafficking in persons, activities related to the proliferation of weapons of mass destruction, activity that violates or threatens to violate human rights or principles of national sovereignty, or money laundering to conceal any such activity. In this regard, and although not dispositive, the Corporation may consider the appearance of the Customer, its owner or a related person or entity on a United Nations or domestic or foreign governmental sanction list that identifies persons or entities believed to engage in such illicit activity; or
14. The Corporation has reason to believe that not terminating such Participation would be harmful to the Corporation's goodwill or reputation.

The Corporation may terminate any PTA Program and the associated PTA Agreement (a) upon ninety (90) days' notice, if the Corporation discontinues such PTA Program in one or more of the countries in a PTA Customer's Area of Use; (b) upon notice, if the Corporation is required to obtain a new license in order to provide such PTA Program in a PTA Customer's Area of Use; (c) upon thirty (30) or fewer days' notice, if required by applicable law or the relevant governing authority, if the Corporation is required by such law or governing authority to cease providing such PTA Program in one or more countries in the PTA Customer's Area of Use; (d) upon notice, if the Corporation determines in its sole discretion that a PTA Program cannot be provided in

compliance with applicable law or governing authority, or if applicable, Non-Mastercard Systems and Network Standards; or (e) upon notice, if the Corporation has received a claim or notice alleging that such PTA Program infringes or violates a third party's intellectual property right.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

1.13.3 Termination for Provision of Inaccurate Information

The Corporation, at any time and by written notice, may require a Customer to confirm the accuracy of information provided by the Customer to the Corporation pursuant to the Standards or the terms of the Licenses.

Within 30 days of receipt of such a notice, the Customer must demonstrate to the satisfaction of the Corporation that either: (i) the information provided was accurate; or (ii) with respect to any inaccurate information, such inaccurate information was provided to the Corporation through inadvertence or with a reasonable belief as to its truth and provide information sufficient to correct such inaccuracy. Without limiting any Corporation right of immediate termination set forth in Rule 1.13.2, the Corporation may terminate a Customer's Participation and/or Licenses without further notice should the Corporation determine that the Customer has failed to make a sufficient showing under (i) or (ii) above, that any Customer representation or demonstration under (i) or (ii) above was false, or should the Customer otherwise fail to comply with the obligations set forth in this Rule.

1.13.4 Rights, Liabilities, and Obligations of a Terminated Customer

All of the following apply with respect to a terminated Customer.

1. Except as otherwise set forth in the Standards, a terminated Customer has no right to use any Mark or to otherwise engage or participate in any Activity or Digital Activity. A terminated Customer must immediately cease its use of all Marks and must ensure that such Marks are no longer used by any of the following:
   a. The Customer's Merchants;
   b. Any Affiliate Sponsored by a terminated Principal or Association;
   c. Any Service Providers that performs any service described in Rule 7.1, which service directly or indirectly supports a Program of a terminated Principal or Association and/or of any Affiliate Sponsored by a terminated Principal or Association;
   d. Merchants of an Affiliate Sponsored by a terminated Principal or Association; or
   e. Any other entity or person acting to provide, directly or indirectly, service related to Activity or Digital Activity undertaken pursuant to the authority or purported authority of the terminated Customer.
2. A terminated Customer is not entitled to any refund of dues, fees, assessments, or other payments and remains liable for, and must promptly pay to the Corporation (a) any and all applicable dues, fees, assessments, or other charges as provided in the Standards and (b) all other charges, debts, liabilities, and other amounts arising or owed in connection with the Customer's Activities or Digital Activities, whether arising, due, accrued, or owing before or after termination.
3. The terminated Customer must promptly cancel all Cards then outstanding that were issued by the terminated Customer and, if the terminated Customer is a Principal or

Association, by all of that Customer's Sponsored Affiliates. All Payment Applications resident on Chip Cards issued by a terminated Customer must be eradicated or disabled no more than six months after the effective date of termination. With respect to any such Card not used during the six-month period, the Issuer must block all Payment Applications the first time the Card goes online.

4. The terminated Customer must promptly cause all of its Cardholders and, if the terminated Customer is a Principal or Association, the Cardholders of its Sponsored Affiliates to be notified of the cancellation of Cards in writing. When the PTA Program includes PTA Transactions that are branded Mastercard or Maestro, the terminated PTA Customer must promptly cause all of its Account Holders and, if the terminated PTA Customer is a Principal or Association, must promptly cause the Account Holders of its Sponsored Affiliates to be notified of the termination of participation of PTA Accounts in the PTA Program in writing. Such notice must be in a form and substance satisfactory to the Corporation.
5. A terminated Customer must give prompt notice of its termination to any Merchants the Customer has authorized to honor Cards and/or PTA Transactions. If any such Merchant wishes to continue to accept Cards and/or PTA Transactions, the terminated Customer must cooperate with the Corporation and other Customers in facilitating the transfer of such Merchant to another Customer.
6. If a terminated Customer does not take an action that this Rule or any other Standard or that the Corporation otherwise requires, the Corporation may take any such required action without prior notice to the terminated Customer on behalf of and at the expense of the Customer.
7. If a Principal or Association that Sponsors one or more Affiliates terminates its Participation, such Principal or Association must cause each of its Sponsored Affiliates to take the actions required of a terminated Customer under this Rule, unless and to the extent that any such Affiliate becomes an Affiliate Sponsored by a different Principal or Association within a period of time acceptable to the Corporation.
8. If an Affiliate terminates its Licenses or its Sponsorship by a Principal or Association, the Sponsoring Principal or Association must cause the Affiliate to take the actions required of a terminated Customer under this Rule. If that Affiliate fails to so comply, the Corporation may take any action that this Rule requires without notice to the Affiliate or the Sponsoring Principal or Association on behalf of and at the expense of the Sponsoring Principal or Association.
9. If an Affiliate Sponsored by a Principal or Association ceases to be so Sponsored by that Principal or Association, such Principal or Association nonetheless is obligated, pursuant to and in accordance with the Standards, to accept from other Customers (a) the records of Transactions arising from the use of Cards issued by that formerly Sponsored Affiliate and whether such Transactions arise before or after the cessation of the Sponsorship and/or (b) the records of PTA Transactions arising from the use of PTA Accounts established by that formerly Sponsored Affiliate and whether such PTA Transactions arise before or after the cessation of the Sponsorship.
10. A terminated Customer has no right to present records of Transactions or PTA Transactions effected after the date of termination to any other Customer, except as permitted by the Standards.

11. A terminated Customer continues to have the rights and obligations set forth in the Standards and Licenses with respect to its use of the Marks and conduct of Activity until such time as the Corporation determines such rights or obligations or both cease.
12. A terminated Customer has a continuing obligation to provide promptly to the Corporation, on request, Customer Reports and any other information about Activity or Digital Activity.
13. A terminated Customer must, at the option of the Corporation, immediately either destroy, or take such steps as the Corporation may require regarding, all confidential and proprietary information of the Corporation in any form previously received as a Customer.
14. The Corporation may continue the Participation and Licenses or Digital Activity Agreements or PTA Agreements, as the case may be, of a terminated Customer for purposes of the orderly winding down or transfer of the terminated Customer's business. Such continuation of Participation and Licenses or Digital Activity Agreements or PTA Agreements is subject to such terms as may be required by the Corporation.

Chapter 2 Standards and Conduct of Activity and Digital Activity

This chapter contains Rules relating to the Standards and the conduct of Activity and Digital Activity.

2.1 Standards

From time to time, the Corporation promulgates Standards governing the conduct of Customers and Activity or Digital Activity.

The Corporation has the sole right to interpret and enforce the Standards.

The Corporation has the right, but not the obligation, to resolve any disagreement or dispute, as applicable, between or among Customers including, but not limited to, any disagreement or dispute, as applicable, involving the Corporation, the Standards, or the Customers' respective Activities or Digital Activities, and any such resolution by the Corporation is final and not subject to appeal, review, or other challenge. In resolving disagreements or disputes, as applicable, between or among Customers, or in applying its Standards to Customers, the Corporation may deviate from any process in the Standards or that the Corporation otherwise applies, and may implement an alternative process, if an event, including, without limitation, an account data compromise event, is, in the sole judgment of the Corporation, of sufficient scope, complexity and/or magnitude to warrant such deviation. The Corporation will exercise its discretion to deviate from its Standards only in circumstances the Corporation determines to be extraordinary. Any decision to alter or suspend the application of any process(es) will not be subject to appeal, review, or other challenge.

2.1.1 Variances

A variance is the consent by the Corporation for a Customer and/or a Network Enablement Partner to act other than in accordance with a Standard. Only a Customer or a Network Enablement Partner may request a variance.

Any such request must specify the Rules or other Standards for which a variance is sought. The request must be submitted to the Corporation in writing, together with a statement of the reason for the request.

2.1.2 Failure to Comply with a Standard

Failure to comply with any Standard adversely affects the Corporation and its Customers and undermines the integrity of the Mastercard system.

Accordingly, a Customer that fails to comply with any Standard is subject to assessments ("noncompliance assessments") as set forth in the Standards.

In lieu of, or in addition to, the imposition of a noncompliance assessment, the Corporation, in its sole discretion, may require a Customer to take such action and the Corporation itself may take such action as the Corporation deems necessary or appropriate to ensure compliance with the Standards and safeguard the integrity of the Mastercard system. In the exercise of such discretion, the Corporation may consider the nature, willfulness, number and frequency of occurrences and possible consequences resulting from a failure to comply with any Standard. The Corporation may provide notice and limited time to cure such noncompliance before imposing a noncompliance assessment.

The Corporation reserves the right to limit, suspend or terminate a Customer's Participation and/or Licenses or to amend the rights, obligations, or both of the Customer, whether set forth

in a License or otherwise, if that Customer does not comply with any Standards or with any decision of the Corporation with regard to the interpretation and enforcement of any Standards.

2.1.3 Noncompliance Categories

From time to time, the Corporation establishes programs that address instances of noncompliance with particular Standards.

Every instance of noncompliance with a Standard not addressed by such a program falls into at least one of the following three compliance categories.

Category A—Payment System Integrity

Category A noncompliance affects payment system integrity. The Corporation has the authority to impose monetary noncompliance assessments for Category A noncompliance. "Payment system integrity" violations include, but are not limited to, noncompliance involving License or Payment Transfer Activity (PTA) Agreement requirements, Merchant, Account Holder, and ATM owner signing and monitoring requirements, and the protection of Card, Account, Transaction, PTA Account, and PTA Transaction information.

Category B—Visible to Customers

Category B noncompliance addresses conduct that is visible to the customers of Issuers and/or Acquirers and/or PTA Customers. The Corporation has the authority to impose monetary noncompliance assessments for Category B noncompliance or, in the alternative, may provide notice and a limited time to cure such noncompliance before imposing monetary assessments. "Visible to customers" violations include, but are not limited to, noncompliance involving the use of the Marks, the selective authorization of Transactions, identification of the Merchant at the POI, the setting of minimum and maximum Transaction amounts, the payment of Merchants and Submerchants for Transactions or the payment of Merchants, Receiving Account Holders, and Submerchants for PTA Transactions (and the timing of posting such PTA Transactions), Transaction and PTA Transaction (if applicable) receipt requirements, and ATM Access Fee notices.

Category C—Efficiency and Operational Performance

Category C noncompliance addresses efficiency and operational performance. The Corporation has the authority to impose monetary noncompliance assessments for Category C noncompliance or, in the alternative, may provide notice and a limited time to cure such noncompliance before imposing monetary assessments. "Efficiency and operational performance" violations include, but are not limited to, noncompliance involving presentment of Transactions or, if applicable, PTA Transactions within the required time frame, supplying Merchants with materials required for Transaction processing, Card capture at the ATM, Card fees and reporting procedures, and the obligation to provide the Corporation with requested information.

2.1.4 Noncompliance Assessments

The following schedule pertains to any Standard that does not have an established compliance program. The Corporation may deviate from this schedule at any time.

Compliance Category	Assessment Type	Assessment Description
A	Per violation	Up to USD 25,000 for the first violation Up to USD 50,000 for the second violation within 12 months Up to USD 75,000 for the third violation within 12 months Up to USD 100,000 per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction or PTA Transaction)	Up to USD 2,500 per occurrence for the first 30 days Up to USD 5,000 per occurrence for days 31–60 Up to USD 10,000 per occurrence for days 61–90 Up to USD 20,000 per occurrence for subsequent violations
	Variable occurrence (by number of Cards or PTA Accounts)	Up to USD 0.50 per Card or PTA Account Minimum USD 1,000 per month per Portfolio or PTA Account Portfolio No maximum per month per Portfolio or per all Portfolios or PTA Account Portfolio(s)
B	Per violation	Up to USD 20,000 for the first violation Up to USD 30,000 for the second violation within 12 months Up to USD 60,000 for the third violation within 12 months Up to USD 100,000 per violation for the fourth and subsequent violations within 12 months

Compliance Category	Assessment Type	Assessment Description
	Variable occurrence (by device or Transaction or PTA Transaction)	Up to USD 1,000 per occurrence for the first 30 days Up to USD 2,000 per occurrence for days 31–60 Up to USD 4,000 per occurrence for days 61–90 Up to USD 8,000 per occurrence for subsequent violations
	Variable occurrence (by number of Cards or PTA Accounts)	Up to USD 0.30 per Card or PTA Account Minimum USD 1,000 per month per Portfolio or PTA Account Portfolio Maximum USD 20,000 per month per Portfolio or PTA Account Portfolio Maximum USD 40,000 per month per all Portfolios or PTA Account Portfolio(s)
C	Per violation	Up to USD 15,000 for the first violation Up to USD 25,000 for the second violation within 12 months Up to USD 50,000 for the third violation within 12 months Up to USD 75,000 per violation for the fourth and subsequent violations within 12 months
	Variable occurrence (by device or Transaction or PTA Transaction)	Up to USD 1,000 per occurrence for the first 30 days Up to USD 2,000 per occurrence for days 31–60 Up to USD 4,000 per occurrence for days 61–90 Up to USD 8,000 per occurrence for subsequent violations

Compliance Category	Assessment Type	Assessment Description
	Variable occurrence (by number of Cards or PTA Accounts)	Up to USD 0.15 per Card or PTA Account Minimum USD 1,000 per month per Portfolio or PTA Account Portfolio Maximum USD 10,000 per month per Portfolio or PTA Account Portfolio Maximum USD 20,000 per month per all Portfolios or PTA Account Portfolio(s)

In the above table, all days refer to calendar days and violations of a Standard are tracked on a rolling 12-month basis.

2.1.5 Certification

A senior executive officer of each Principal, Association, Affiliate, and Digital Activity Customer must, if requested by the Corporation, promptly certify in writing to the Corporation the status of compliance or noncompliance with any Standard by the Customer or in the case of a Principal or Association, by any of its Sponsored Affiliates.

2.1.6 Review Process

A Customer may request that the Chief Franchise Officer of the Corporation review an assessment imposed by the Corporation for noncompliance with a Standard.

Such a request must be submitted in English by email from the email address of the Customer's principal contact as listed in the My Company Manager application on Mastercard Connect™ to franchise.appeals@mastercard.com no later than 30 calendar days after the date of the disputed assessment.

The Corporation may assess a USD 500 fee to consider and act on a request for review of a noncompliance assessment.

2.1.7 Resolution of Review Request

When a Customer requests review of an assessment for noncompliance with a Standard, the Chief Franchise Officer of the Corporation may take such action as he or she deems necessary or appropriate or may elect not to act.

The Chief Franchise Officer may delegate authority to act or not to act with respect to any particular matter or type of matter.

If the Chief Franchise Officer or his or her designee elects to conduct further inquiry into the matter, each Customer must cooperate promptly and fully. If the Chief Franchise Officer or his

or her designee makes a recommendation of action to resolve the matter, such recommendation is final and not subject to further review or other action.

2.1.8 Rules Applicable to Intracountry Transactions

NOTE: Rules on this subject appear in the "Europe Region" chapter.

2.2 Conduct of Activity and Digital Activity

Each Customer, at all times, must conduct Activity and Digital Activity in compliance with the Standards and with all applicable laws and regulations.

A Customer is not required to undertake any act that is unambiguously prohibited by applicable law or regulation. If a Customer is unable to comply with a Standard because of applicable law or regulation, then the Corporation may require that such Customer undertake some other form of permissible Activity.

If a party other than a Customer files a claim against a Customer concerning the Customer's Activity or Digital Activity, the Corporation must be informed thereof by the Customer. The Corporation is entitled but not obliged to intervene in the case.

2.2.1 Customer Responsibilities

At all times, each Customer must:

1. Be entirely responsible for and Control all aspects of its Activities and Digital Activities, and the establishment and enforcement of all management and operating policies applicable to its Activities and Digital Activities, in accordance with the Standards;
2. Not transfer or assign any part or all of such responsibility and Control or in any way limit its responsibility or Control;
3. Ensure that all policies applicable to its Activities and Digital Activities conform to the Standards and comply with all applicable laws and government and local authority regulations;
4. Conduct meaningful and ongoing monitoring to ensure compliance with all of the responsibilities set forth in this Rule, and be able to demonstrate such monitoring and compliance upon request of the Corporation in accordance with the Standards, including without limitation, Rule 2.5;
5. Ensure that each of its employees, agents and contractors complies with all anti-bribery and corruption laws applicable to business dealings and any implementing regulations in respect of any such laws. The Customer must not, in connection with its business activities involving the Corporation: (i) make, promise, or offer to make any payment or transfer of anything of value or any other advantage directly or indirectly through a representative, intermediary, agent, or otherwise to any government official or to any other person for the purpose of improperly influencing any act, omission to act, or decision of such official or individual or securing an improper advantage to assist the Customer and/or the Corporation in obtaining or retaining business; nor (ii) accept anything of value from any third party seeking to

influence any act or decision of the Customer or in order to secure an improper advantage to that third party.
For purposes of this Rule, "government official" is defined as any employee or officer of a government of a country, state, or region, including any federal, regional, or local government or department, agency, or enterprise owned or controlled by such government; any official of a political party; any official or employee of a public international organization; any person acting in an official capacity for, or on behalf of, such entities; and any candidate for political office.

6. Maintain a significant economic interest in each of its Activities and Digital Activities;
7. Engage in Activities and Digital Activities at a scale or volume of operations consistent with the business plans accepted by the Corporation in connection with the application to be a Customer or application for a License, a Digital Activity Agreement, and/or PTA Agreement, as the case may be;
8. Promptly update information set forth in its application, business plans and other materials previously provided to the Corporation in the event of a significant change to the accuracy or completeness of any of the information contained therein and, separately, upon request of the Corporation;
9. Promptly inform the Corporation should the Customer become unable for any reason to engage in Activity or Digital Activity in accordance with both the Standards and the laws and government and local authority regulations of any country (or any subdivision thereof) in which the Customer is Licensed to engage in Activity or approved to conduct Digital Activity;
10. Comply with such other requirements as the Corporation may establish, in its sole discretion, in connection with the Customer's Activity and Digital Activity.
11. Ensure that data elements, subelements and subfields of Transaction Data are only disclosed by the Customer, its Service Providers or its employees, agents and contractors and personnel (a) solely for the purpose of carrying out the Customer's Activities or Digital Activities, as the case may be, for Category One Transaction Data and (b) for the specific purpose for which it was provided as set forth in the applicable Standards for Category Two Transaction Data. The Corporation assigns a category (e.g., Category One Transaction Data or Category Two Transaction Data) to each data element, subelement and subfield. Category assignments for Transaction Data are available in the *Customer Interface Specification* manual, the *IPM Clearing Formats* manual and the *Single Message System Specifications* manual, or other applicable Standards.

2.2.2 Obligations of a Sponsor

Each Principal and Association that Sponsors one or more Affiliates must cause each such Affiliate to comply with all Standards applicable to the Activity of that Affiliate.

Each Sponsor is liable to the Corporation and to all other Customers for all Activities of each of its Sponsored Affiliates and for any failure by any such Sponsored Affiliate to comply with a Standard or with applicable law or regulation.

2.2.3 Affiliates

Except to the extent any liability or obligation arising under a Standard has been satisfied by a Sponsor, each Affiliate is responsible for the liabilities and obligations arising out of or in connection with its Activities, regardless of any:

1. Action taken by such Affiliate to satisfy such liability or obligation with, through or by a Sponsor or former Sponsor of such Affiliate, or
2. Agreement between any Sponsor and such Affiliate.

In accordance with the Standards and in compliance with all applicable laws and regulations, each Sponsor will have access to and may use or otherwise process its Sponsored Affiliates' Confidential Information and Confidential Transaction Data (as these terms are defined in Rule 3.10) in connection with authorization, settlement, clearing, fraud reporting, chargebacks, billing, and other related activities.

2.2.4 Financial Soundness

Each Customer must conduct all Activity and otherwise operate in a manner that is financially sound and so as to avoid risk to the Corporation and to other Customers.

A Customer must promptly report to the Corporation any materially adverse financial condition or discrepancy or suspected materially adverse financial condition or discrepancy relating to the Customer or, in the case of a Principal or Association, any Sponsored Affiliate.

The Customer must refer or, if applicable, cause the Affiliate to refer such condition or discrepancy to independent certified public accountants or another person or firm satisfactory to the Corporation for evaluation and recommendation as to remedial action, and promptly provide to the Corporation a copy of such evaluation and recommendation after receipt thereof.

2.2.5 Mastercard Acquirers

NOTE: A Rule on this subject appears in the "Additional U.S. Region and U.S. Territory Rules" chapter.

2.2.6 Compliance

From time to time, the Corporation may develop means and apply criteria to evaluate a Customer's compliance with Rule 2.2.

Each Customer must fully cooperate with any effort by the Corporation and the Corporation's representatives to evaluate a Customer's compliance with Rule 2.2.

In the event that the Corporation determines that a Customer is not complying or may not on an ongoing basis comply with the requirements of Rule 2.2, the Corporation may:

1. Impose special terms upon the Customer as the Corporation deems necessary or appropriate until each condition or discrepancy is resolved to the Corporation's satisfaction so as to enable the Customer to be and to remain in full compliance with Rule 2.2, or
2. Require the Customer to withdraw its Participation.

2.2.7 Information Security Program

A Customer and the Corporation, where relevant, must implement and maintain a comprehensive written information security program in accordance with applicable privacy and data protection requirements, including Rule 3.13, that includes technical, physical, administrative, and organizational safeguards designed to:

1. Ensure the security and confidentiality of confidential information of the Corporation and Personal Data;
2. Protect against any anticipated threats or hazards to the security, confidentiality, and integrity of Personal Data;
3. Protect against any actual or suspected unauthorized processing, loss, or unauthorized acquisition of any Personal Data; and
4. Ensure the proper and secure disposal of Personal Data.

A Customer's information security program must regularly test or monitor the effectiveness of the safeguards stated in this Rule.

A Customer and the Corporation must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation.

2.3 Indemnity and Limitation of Liability

Each Customer (each, for the purposes of this Rule, an "Indemnifying Customer") must protect, indemnify, and hold harmless the Corporation and the Corporation's parent and subsidiaries and affiliated entities, and each of the directors, officers, employees and agents of the Corporation and the Corporation's parent and subsidiaries and affiliated entities from any actual or threatened claim, demand, obligation, loss, cost, liability and/or expense (including, without limitation, actual attorneys' fees, costs of investigation, and disbursements) resulting from and/or arising in connection with, any act or omission of the Indemnifying Customer, its subsidiaries, or any person associated with the Indemnifying Customer or its subsidiaries (including, without limitation, such Indemnifying Customer's directors, officers, employees and agents, all direct and indirect parents, subsidiaries, and affiliates of the Indemnifying Customer, the Indemnifying Customer's customers in connection with all types of Activity and/or Digital Activity and/or other business, and the Indemnifying Customer's suppliers, including, without limitation, Service Providers, Card production vendors, and other persons acting for, or in connection with, the Indemnifying Customer or a Merchant or other entity for which the Indemnifying Customer acquires Transactions, Account Holder, Merchant, or other entity for which the Indemnifying Customer originates or receives PTA Transactions, or any such Merchant's, Account Holder's, or entity's employees, representatives, agents, suppliers, or customers, including but not limited to any Data Storage Entity [DSE]) with respect to, or relating to:

1. Any Programs and/or other Activities and/or Digital Activities of the Indemnifying Customer;

2. Any programs and/or activities of any person associated with the Indemnifying Customer and/or its subsidiaries;
3. The compliance or noncompliance with the Standards by the Indemnifying Customer;
4. The compliance or noncompliance with the Standards by any person associated with the Indemnifying Customer and its subsidiaries;
5. Any other activity of the Indemnifying Customer;
6. Direct or indirect access to and/or use of the Interchange System (it being understood that the Corporation does not represent or warrant that the Interchange System or any part thereof is or will be defect-free or error-free and that each Customer chooses to access and use the Interchange System at the Customer's sole risk and at no risk to the Corporation);
7. Any other activity and any omission of the Indemnifying Customer and any activity and any omission of any person associated with the Indemnifying Customer, its subsidiaries, or both, including but not limited to any activity that used and/or otherwise involved any of the Marks or other assets;
8. Any failure of another Customer to perform as required by the Standards or applicable law; or
9. The Corporation's interpretation, enforcement, or failure to enforce any Standards.

The Corporation does not represent or warrant that the Interchange System or any other system, process or activity administered, operated, controlled or provided by or on behalf of the Corporation (collectively, for purposes of this section, the "Systems") is free of defect and/or mistake and, unless otherwise specifically stated in the Standards or in a writing executed by and between the Corporation and a Customer, the Systems are provided on an "as-is" basis and without any express or implied warranty of any type, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose or non-infringement of third party intellectual property rights. IN NO EVENT WILL THE CORPORATION BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, FOR LOSS OF PROFITS, OR ANY OTHER COST OR EXPENSE INCURRED BY A CUSTOMER OR ANY THIRD PARTY ARISING FROM OR RELATED TO USE OR RECEIPT OF THE SYSTEMS, WHETHER IN AN ACTION IN CONTRACT OR IN TORT, AND EVEN IF THE CUSTOMER OR ANY THIRD PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EACH CUSTOMER ASSUMES THE ENTIRE RISK OF USE OR RECEIPT OF THE SYSTEMS.

Only in the event the limitation of liability set forth in the immediately preceding paragraph is deemed by a court of competent jurisdiction to be contrary to applicable law, the total liability, in aggregate, of the Corporation to a Customer and anyone claiming by or through the Customer, for any and all claims, losses, costs or damages, including attorneys' fees and costs and expert-witness fees and costs of any nature whatsoever or claims expenses resulting from or in any way related to the Systems shall not exceed the total compensation received by the Corporation from the Customer for the particular use or receipt of the Systems during the 12 months ending on the date that the Corporation was advised by the Customer of the Systems concern or the total amount of USD 250,000.00, whichever is less. It is intended that this limitation apply to any and all liability or cause of action however alleged or arising; to the fullest extent permitted by law; unless otherwise prohibited by law; and notwithstanding any other provision of the Standards.

A payment or credit by the Corporation to or for the benefit of a Customer that is not required to be made by the Standards will not be construed to be a waiver or modification of any Standard by the Corporation. A failure or delay by the Corporation to enforce any Standard or exercise any right of the Corporation set forth in the Standards will not be construed to be a waiver or modification of the Standard or of any of the Corporation's rights therein.

2.4 Choice of Laws

The substantive laws of the State of New York govern all disputes involving the Corporation, the Standards, and/or Customers and Activity and Digital Activity without regard to conflicts.

Any action initiated by a Customer regarding and/or involving the Corporation, the Standards and/or any Customer and Activity and Digital Activity must be brought, if at all, only in the United States District Court for the Southern District of New York or the New York Supreme Court for the County of Westchester, and any Customer involved in an action hereby submits to the jurisdiction of such courts and waives any claim of lack of personal jurisdiction, improper venue, and *forum non conveniens*.

This provision in no way limits or otherwise impacts the Corporation's authority described in Rule 2.1. Each Customer agrees that the Standards are construed under, and governed by, the substantive laws of the State of New York without regard to conflicts.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

2.5 Examination and Audit

The Corporation reserves the right to conduct an examination or audit of any Customer and Customer information to ensure full compliance with the Standards.

Any such examination or audit is at the expense of the Customer, and a copy of the examination or audit results must be provided promptly to the Corporation upon request.

Further, the Corporation, at any time and whether or not a Customer is subject to periodic examination or audit or other oversight by banking regulatory authorities of a government and government and local authorities, and at the Customer's sole expense, may require that Customer to be subjected to an examination and/or audit and/or periodic examination and/or periodic audit by a firm of independent certified accountants or by any other person or entity satisfactory to the Corporation.

A Customer may not engage in any conduct that could or would impair the completeness, accuracy or objectivity of any aspect of such an examination or audit and may not engage in any conduct that could or would influence or undermine the independence, reliability or integrity of the examination or audit. A Customer must cooperate fully and promptly in and with the examination or audit and must consent to unimpeded disclosure of information to the Corporation by the auditor.

If as a result of an examination or audit of a Customer, the Corporation determines that the Customer must take certain actions, the Customer must take such actions as directed by the Corporation.

Chapter 3 Customer Obligations

This chapter contains Rules relating to Customer obligations.

3.1 Obligation to Issue Mastercard Cards

Each Principal and Association Licensed to use the Mastercard Marks, together with its Sponsored Affiliates, must have issued and outstanding a reasonable number of Mastercard Cards based on such criteria as the Corporation may deem appropriate from time to time.

In addition to any other action that the Corporation deems appropriate, such a Principal or Association that does not issue and have outstanding the requisite number of Mastercard Cards will be assessed an additional 20 percent of the assessment paid on its acquiring volume for each year in which the Card-issuing shortfall exists.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "Latin America and the Caribbean Region," "Middle East/Africa Region," and "United States Region" chapters.

3.2 Responsibility for Transactions

Each Principal and Association is responsible to the Corporation and to all other Customers for Transactions arising from the use of the ICAs and BINs that the Corporation assigns to the Principal or Association, and for any Cards that the Principal or Association or any of its Sponsored Affiliates, if any, has issued.

A Customer must use ICAs and BINs only in accordance with the Standards.

Neither a Principal, an Association, nor any of its Sponsored Affiliates may use the Principal's or Association's ICAs or BINs to issue Cards or acquire Transactions other than as specified by the Corporation.

Each Principal and Association must provide to the Corporation all information and material related to ICAs and BINs usage, promptly following any request from the Corporation, including identification of any Corporation Asset used by a Sponsored Affiliate or Sponsored Program Manager.

Payment Transfer Activity Variation

The first and third paragraphs in the Rule on this subject, as it applies to Payment Transfer Activity (PTA), are revised and restated as follows.

Each PTA Customer is responsible to the Corporation and to all other Customers for PTA Transactions arising from or otherwise involving its Account Holders.

Neither a Principal, an Association, nor any of its Sponsored Affiliates may use the Principal's or Association's ICAs or BINs for PTA Transactions other than as specified by the Corporation.

3.3 Transaction Requirements

In accordance with the Standards, each Customer must comply with each of the following requirements.

1. Accept and present to the Issuer records of Transactions arising from the use of a Card issued by any other Customer at any POI location the Customer has authorized to honor Cards;
2. Accept and pay for Transactions received from another Customer arising from the use of any Card issued by it. If an Affiliate ceases to be Sponsored by a Principal or Association, the Principal or Association remains obligated to other Customers to accept and pay for Transactions arising from the use of Cards issued by that Affiliate;
3. Maintain a functional 24-hour-per-day operating connection to the Interchange System, either directly or by means of a Service Provider operating on its behalf, and not force any other Customer wishing to operate multilaterally using the Interchange System into bilateral agreements;
4. Provide valid, accurate, complete, unaltered, and consistent data in all authorization and clearing Transaction messages; and
5. Ensure that each Cross-border Transaction is processed through the Interchange System (a "Processed Transaction," as described in the Definitions section), unless the Customer has applied for and received the consent of the Corporation to process Cross-border Transactions through other means. In the event applicable law prevents a Customer from processing Cross-border Transactions through the Interchange System, the Customer must promptly notify the Corporation and undertake an alternative means of processing Cross-border Transactions that, in the opinion of the Corporation, will not damage the goodwill or reputation of the Corporation or of any Mark and that is otherwise satisfactory to the Corporation.

If Cross-border Transactions are not processed through the Interchange System, either the Issuer or the Acquirer or both must promptly provide the Corporation with such Customer Reports pertaining to such Cross-border Transactions and the processing thereof as the Corporation may require from time to time. Such Customer Reports and all information set forth therein shall be subject to Rule 3.10.

In the event that a Customer is party to a bilateral or multilateral arrangement pertaining to the processing of Cross-border Transactions established before 1 June 2009 and such Customer has not applied for and received prior written approval by the Corporation of such arrangement, then such Customer must:

1. Register such bilateral or multilateral arrangement with the Corporation;
2. Provide the Corporation information deemed by the Corporation to be sufficient to determine whether such arrangement will damage the goodwill or reputation of the Corporation or of any Mark or is otherwise unsatisfactory to the Corporation; and
3. If the Corporation deems such arrangement to be unsatisfactory, work with the Corporation in good faith and in a timely manner to effect such changes as may be necessary or appropriate to render the arrangement satisfactory to the Corporation.

Refer to the *Single Message System Specifications*, *Customer Interface Specification* and *IPM Clearing Formats* manuals for technical requirements relating to Processed Transactions. Refer to the *Data Integrity Monitoring Program* manual for information about the Corporation's monitoring of Processed Transaction data.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "United States Region," and "Additional U.S. Region and U.S. Territory Rules" chapters.

Payment Transfer Activity Variation

The Rule on this subject, as it applies to Payment Transfer Activity, is revised and restated as follows.

In accordance with the Standards, each PTA Customer must comply with each of the following requirements.

1. Maintain a functional 24-hour-per-day operating connection to the applicable Corporation System, either directly or by means of a Service Provider operating on its behalf, and not force any other PTA Customer wishing to operate multilaterally using the Corporation System into bilateral agreements; and
2. When conducting Payment Transfer Activity, provide valid, accurate, complete, unaltered, and consistent data in connection with PTA Transactions, including, without limitation, PTA Account information, and all initiation and clearing PTA Transaction messages and other information.

3.4 Authorization Service

Each Principal and Association must provide, at its own expense and in compliance with the Standards, including but not limited to those set forth in the *Transaction Processing Rules* manual:

1. Authorization services with respect to Cards that the Sponsoring Customer and each of its Sponsored Affiliates has issued; and
2. Adequate and reasonable authorization services with respect to its Merchants and those of its Sponsored Affiliates. Each such Merchant must be instructed as to the proper use of such authorization services so as to ensure that Card acceptance and Transaction processing is conducted in compliance with the Standards.

3.5 Non-discrimination—POS Transactions

A Customer must not discriminate against any Merchant with regard to processing and authorizing POS Transactions received.

3.6 Non-discrimination—ATM and Bank Branch Terminal Transactions

Pursuant to the Standards, each Customer must:

1. Honor all valid Cards at each ATM Terminal and Bank Branch Terminal for which it is responsible, in a manner that is no less favorable than the manner in which it honors the cards of any other ATM network in which the Customer participates; and
2. Acquire and process all valid Transactions in a manner that is no less favorable than the manner in which it acquires and processes transactions of any other ATM network in which the Customer takes part.

Except as the Standards permit, a Customer must not discriminate against other Customers of the Corporation as to any of the terms or conditions upon which it honors Cards, or acquires or processes Transactions.

If an Acquirer is expressly permitted by the Corporation or local law to block use of its ATM Terminals to Cards issued by a Customer within the same country, the Acquirer must display notifications accompanying the Marks on or near such ATM Terminals informing the affected Cardholders that their Cards are not accepted.

NOTE: Modifications to this Rule appear in the "Europe Region" chapter.

3.7 Integrity of Brand and Network

A Customer must not directly or indirectly engage in or facilitate any action that is illegal or that, in the opinion of the Corporation and whether or not addressed elsewhere in the Standards, damages or may damage the goodwill or reputation of the Corporation or of any Mark, or damages or may damage the integrity of the Mastercard system, including the Interchange System or other Corporation assets.

Upon request of the Corporation, a Customer will promptly cease engaging in or facilitating any such action.

In addition, a Customer must not place or cause to be placed on any Card or any Terminal or other acceptance device any image, information, application or product that would in any way, directly or indirectly, have or potentially have the effect of diminishing or devaluing the reputation or utility of the Marks, a Card, or any of the Corporation's products, programs, services, networks, or systems.

NOTE: Modifications to this Rule appear in the "United States Region" chapter.

3.8 Fees, Assessments, and Other Payment Obligations

Each Customer is responsible to timely pay to the Corporation all fees, charges, assessments and the like applicable to Activity as may be in effect from time to time, including those set forth in the Pricing and Billing Center on Mastercard Connect™.

If a Customer does not timely pay the Corporation or any other person any amount due under the Standards, then the Corporation has the right, immediately and without providing prior notice to the Customer, to assess and collect from that Customer, on a current basis as the Corporation deems necessary or appropriate, such amount, as well as the actual attorneys' fees and other costs incurred by the Corporation in connection with any effort to collect such amount from that Customer.

The Corporation may assess and collect such amount at any time after the applicable amount becomes due, by any means available to the Corporation, which shall specifically include, by way of example and not limitation:

1. The taking or setoff of funds or other assets of the Customer held by the Corporation;
2. The taking or setoff of funds from any account of the Customer upon which the Corporation is authorized to draw;
3. The taking of funds being paid by the Customer to any other Customer; and
4. The taking of funds due to the Customer from any other Customer.

Each Customer expressly authorizes the Corporation to take the Customer's funds and other assets as authorized by this Rule, and to apply such funds and other assets to any obligation of the Customer to the Corporation or any other person under the Standards, and no Customer shall have any claim against the Corporation or any other person in respect of such conduct by the Corporation.

Each Customer agrees upon demand to promptly execute, acknowledge and deliver to the Corporation such instruments, agreements, lien waivers, releases, and other documents as the Corporation may, from time to time, request in order to exercise its rights under this Rule.

3.8.1 Taxes and Other Charges

Each Customer must pay when due all taxes charged by any country or other jurisdiction in which the Customer conducts Activity with respect to such Activity.

In the event the Corporation is charged taxes or other charges by a country or other jurisdiction as a result of or otherwise directly or indirectly attributable to Activity, the Customer is obligated to reimburse the Corporation the amount of such taxes or other charges. The Corporation may collect such taxes or other charges from the settlement account of the Principal or Association responsible in accordance with the Standards for the Activity that gave rise to the charge.

3.8.2 Maestro and Cirrus Card Fees and Reporting Procedures

A Principal must pay fees based upon the number of Maestro and Cirrus Cards issued by the Principal and its Sponsored Affiliates.

In the case of new Affiliates, a Principal must pay a Card fee effective the month after the first Transaction is submitted for the Affiliate.

On or before 30 September of each year, the Corporation will deliver listings to Principals of each specific IIN that appears on the Corporation's routing tables for each Affiliate Customer. On or before 31 October of each year, Principals must certify, as appearing on a report provided by the Corporation:

1. A count of the number of Maestro and Cirrus Cards that are issued using a specific IIN, or
2. A count of the number of Maestro and Cirrus Accounts that have Cards issued for access using a specific IIN.

A Principal must confirm in writing to the Corporation its certification and the certifications of its Sponsored Affiliates. When a count of the number of Accounts that have Cards issued for access is provided, the Corporation will multiply the number provided by a factor of one and four tenths (1.4) to determine the number of Cards issued.

Card count certifications must be signed by the Principal and reviewed by the auditing department, senior officer, or outside auditing firm of the Principal's Service Provider. After such review, concurrence with the Card count certification or the method used to determine the Card count must be provided on the Corporation reports.

3.9 Obligation of Customer to Provide Information

Upon request by the Corporation, and subject to applicable law or regulation, a Customer must complete and timely deliver accurate Customer Reports to the Corporation or to the Corporation's designee, provided that compliance with the foregoing obligation does not require a Customer to furnish any information, the disclosure of which, in the opinion of this Corporation's legal counsel, is likely to create a significant potential legal risk to this Corporation and/or its Customers.

To the extent that a Customer is obligated to provide a Customer Report to the Corporation that the Customer deems to disclose proprietary information of the Customer, such information will be treated by the Corporation with the degree of care deemed appropriate by the Corporation to maintain its confidentiality.

As an example of a Customer Report, each Acquirer must provide Transaction Data to the Corporation in such form and manner as the Corporation may require.

By way of example and not limitation, the Corporation requires such Customer Reports of Transaction Data pursuant to the Global Collection Only (GCO) Data Collection Program and the Quarterly Mastercard Report (QMR).

Each Principal and Association must provide the Corporation with current Customer contact information for itself and on behalf of its Sponsored Affiliates, including mailing addresses, air express/hand delivery addresses, telephone numbers, fax numbers, and email addresses.

3.10 Confidential Information of Customers

The Corporation and its parents, subsidiaries and affiliates (herein collectively referred to as Mastercard) may use and disclose both Confidential Information and Confidential Transaction Data in compliance with applicable law and as provided herein.

For purposes of this Rule 3.10:

- "Confidential Information" means any information of any nature that comes into the possession or under the control of Mastercard, whether temporarily or permanently and whether directly or indirectly, resulting from Activity or Digital Activity or any service provided by or product of Mastercard and which information is deemed by a person other than Mastercard (including, by way of example and not limitation, a Customer or Merchant or Cardholder) to be confidential information of such person; and
- "Confidential Transaction Data" means any information provided to Mastercard by a Customer or Merchant if that information enables Mastercard to determine an individual's identity or includes an Account PAN, Payment Account Reference (PAR) value, or Token.

Mastercard may use or disclose Confidential Information and Confidential Transaction Data only as follows:

1. For the benefit of the Customer supplying the information to support the Customer's Program and/or Activities;
2. As may be appropriate to Mastercard's staff, accountants, auditors, or counsel;
3. As may be required or requested by any judicial process or governmental agency having or claiming jurisdiction over Mastercard;
4. As required for processing Transactions, including authorization, clearing, and settlement;
5. For accounting, auditing, billing, reconciliation, and collection activities;
6. For the purpose of processing and/or resolving chargebacks or other disputes;
7. For the purpose of protecting against or preventing actual or potential fraud, unauthorized transactions, claims, or other liability, including to third parties providing these services;
8. For the purpose of managing risk exposures, franchise quality, and compliance with the Standards;
9. For the purpose of providing products or services to Customers or other third parties, except that any Confidential Transaction Data provided in such products or services will only be provided to a Customer and will consist solely of Confidential Transaction Data provided to Mastercard by that Customer;
10. For the purpose of administering sweepstakes, contests, or other marketing promotions;
11. For preparing internal reports for use by Mastercard staff, management, and consultants for the purposes of operating, evaluating, and managing Corporation business;
12. For preparing and furnishing compilations, analyses, and other reports of aggregated information, and anonymizing Confidential Information and/or Confidential Transaction

Data, provided that such compilations, analyses, or other reports do not identify any (i) Customer other than the Customer for which Mastercard prepares the compilation, analysis, or other report or (ii) Cardholder whose Transactions were involved in the preparation of any such compilation, analysis, or other report;

13. For the purpose of complying with applicable legal requirements; or
14. For other purposes for which consent has been provided by the individual to whom the Confidential Information and/or Confidential Transaction Data relates.

Each Customer must ensure that it complies with the Standards and applicable laws and regulations in connection with disclosing any Confidential Transaction Data or Confidential Information to Mastercard to allow the uses and disclosures described herein, including any laws and regulations requiring the Customer to provide notices to individuals about information practices or to obtain consent from individuals to such practices.

A Customer must provide Confidential Transaction Data to the Corporation or through the Corporation's processes or systems solely as prescribed by the Standards or as otherwise required by the Corporation or applicable law. For example, an Account PAN, PAR, or Token, when provided through the Interchange System, must be submitted in accordance with the technical specifications or other Standards pertaining to the Interchange System or a component thereof.

3.11 Use of Corporation Information by a Customer

The Corporation is not responsible for and disclaims any responsibility for the accuracy, completeness, or timeliness of any information disclosed by the Corporation to a Customer; and the Corporation makes no warranty, express or implied, including, but not limited to, any warranty of merchantability or fitness for any particular purpose with respect to any information disclosed by or on behalf of the Corporation to any Customer or disclosed directly or indirectly to any participant in a Customer's Activity. Each Customer assumes all risk of use of any information disclosed directly or indirectly to a Customer or to any participant in a Customer's Activity by or on behalf of the Corporation.

3.12 Confidential Information of Mastercard

NOTE: A modification to this Rule appears in the "Digital Activity" chapter.

A Customer must not disclose confidential information of the Corporation or its parents, subsidiaries, and affiliates (herein collectively referred to as Mastercard) except:

1. On a need-to-know basis to the Customer's staff, accountants, auditors, or legal counsel subject to standard confidentiality restrictions, or
2. As may be required by any court process or governmental agency having or claiming jurisdiction over the Customer, in which event the Customer must promptly provide written notice of such requirement to the Secretary of the Corporation, and to the extent possible, the Customer must seek confidential treatment by the court or agency.

The obligation set forth herein continues following the termination of a Customer's License. Information provided to a Customer by Mastercard is deemed confidential unless otherwise stated in writing.

A Customer may use confidential or proprietary information and/or trade secrets of Mastercard solely for the purpose of carrying out the Customer's Activities.

3.12.1 Customer Evaluation of Mastercard Technology

From time to time, the Corporation may disclose certain specifications, designs and other technical information or documentation developed by the Corporation ("Mastercard Specifications") to a Customer, solely for the purpose of the Customer's evaluation of such Mastercard Specifications.

Any such disclosure is subject to the following:

1. Each Customer to which the Corporation disclosed any Mastercard Specifications is given a non-exclusive, limited, non-transferable, non-sublicenseable right to reproduce and use such Mastercard Specifications solely for the limited purpose of the Customer's internal evaluation. A Customer may implement prototypes based on the Mastercard Specifications for its internal evaluation purposes in furtherance of such limited purpose, but the Customer may not distribute, license, offer to sell, supply or otherwise provide, demonstrate, or otherwise transfer or disclose, to any third party, any Mastercard Specifications, or any implementation of any Mastercard Specifications.
2. The Corporation does not convey, and no Customer obtains, any rights or license in or to the Mastercard Specifications or any other intellectual property of the Corporation as a result of this Rule, other than as expressly set forth in this Rule. All rights not expressly granted to a Customer with respect to the Mastercard Specifications are retained by the Corporation.
3. Each Customer must treat the Mastercard Specifications and all implementations of the Mastercard Specifications as confidential information of the Corporation subject to Rule 3.12.
4. If a Customer provides any feedback, comments or suggestions to the Corporation regarding the Mastercard Specifications ("Feedback"), the Customer gives the Corporation the right to use such Feedback without restriction.
5. Notwithstanding the provisions of Chapter 7 or any other Standards relating to a Customer's use of Service Providers, a Customer may not use any Service Providers in connection with the Customer's exercise of its rights under this Rule, without the Corporation's express prior written consent, which consent may be withheld or conditioned on other terms and conditions, in the Corporation's sole discretion.

3.13 Privacy and Data Protection

The Corporation and each Customer must comply with Applicable Data Protection Law when Processing Personal Data in the context of the Activity and Digital Activity.

For purposes of this Rule 3.13, the following terms have the meanings set forth below.

Applicable Data Protection Law

All applicable law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation or rule (each as amended and replaced from time to time) which relates to the protection of Data Subject with regards to the Processing of Personal Data to which the Customers and the Corporation are subject, including but not limited to EU Data Protection Law; the California Consumer Privacy Act; the U.S. Gramm-Leach-Bliley Act; Brazil Data Protection Law; the South Africa Protection of Personal Information Act; the Personal Information Protection Law of the People's Republic of China; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws governing the portability and/or cross-border transfer of Personal Data; and all other similar international, federal, state, provincial, and local requirements; each as applicable.

The terms "Data Subject," "Personal Data" and "Processing of Personal Data" are located in Appendix C.

Sub-Processor

The entity engaged by the Customer or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Corporation.

3.13.1 Processing of Personal Data for Purposes of Activity and Digital Activity

A Customer is the organization responsible for complying with the Applicable Data Protection Law in respect of the collection, use and disclosure of Personal Data, including the transfer of Personal Data outside the country of origin, for the purposes of Activity or Digital Activity, and the Corporation acts as an entity that Processes Personal Data on behalf of the Customer for these purposes.

For such activities, the Corporation will only undertake Processing of Personal Data in accordance with the Customer's instructions where they are in compliance with Applicable Data Protection Law and the Standards, and will comply with appropriate organizational, physical and security measures, as applicable to the Corporation under the Applicable Data Protection Law.

NOTE: Modifications to this Rule appears in the the "Asia/Pacific Region", "Europe Region" and the "Latin America and the Caribbean Region" chapters.

3.13.2 Data Subject Notice and Consent

A Customer must ensure that Data Subjects are provided with appropriate notice and, if necessary, have given proper consent in accordance with the Applicable Data Protection Law so that Personal Data relating to them may be collected, used, disclosed, transferred (including any overseas transfers) or otherwise Processed by the applicable Customer and the Corporation for the purposes set forth in the Standards.

NOTE: Modifications to this Rule appears in the the "Asia/Pacific Region", "Europe Region" and the "Latin America and the Caribbean Region" chapters.

3.13.3 Data Subject Rights

In accordance with the Applicable Data Protection Law, a Customer must develop and implement appropriate procedures for handling requests by Data Subjects for access to, correction, deletion and/or other applicable rights of the Data Subjects in relation to Personal Data Processed by the applicable Customer or the Corporation.

The Customer is responsible for responding to such requests. The Corporation will cooperate with the Customer in responding to such requests and will provide access to Personal Data held by the Corporation where required by the Applicable Data Protection Law.

If a request as described above is made by a Data Subject directly to the Corporation, a Customer must cooperate with the Corporation in promptly responding to the request.

NOTE: Modifications to this Rule appears in the the "Asia/Pacific Region", "Europe Region" and the "Latin America and the Caribbean Region" chapters.

3.13.4 Personal Data Accuracy and Data Minimization

A Customer must take reasonable steps to ensure that Personal Data which the Customer provides to the Corporation is:

- accurate, complete, and current;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed; and
- kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed, unless a longer retention is required or allowed under applicable law.

3.13.5 Data Transfers

The Customer authorizes the Corporation to Process Personal Data in accordance with Applicable Data Protection Law in locations outside of the country where the Customer is located (including the United States of America) and/or where the Data Subjects are located (including the United States of America) for the purposes set forth in the Standards.

3.13.6 Sub-Processing

Each Customer authorizes the Corporation to use internal and external Sub-Processors for the purposes of carrying out the Customer's Activity or Digital Activity. The Corporation will require its Sub-Processors, using a written agreement, to comply with Applicable Data Protection Law and with the same obligations as are imposed on the Corporation by the Standards and, where applicable, by Mastercard Binding Corporate Rules.

NOTE: Modifications to this Rule appears in the the "Asia/Pacific Region", "Europe Region" and the "Latin America and the Caribbean Region" chapters.

3.13.7 Returning or Destroying Personal Data

A Customer must destroy, delete, identify, or return (where applicable) any Personal Data it Processes, holds, retains or stores where either upon termination of the Processing services, the Data Subject requests deletion or return of the Personal Data, or the Personal Data is no longer necessary for the purposes set out in the Standards, unless applicable law prevents the Customer from returning or destroying all or part of the Personal Data or requires storage of the Personal Data. Where the Personal Data is retained, the Corporation and/or the Customer will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore.

3.13.8 Regional Variances and Additions

Rules on this subject and modifications to Rule 3.13 and its subsections appear in the "Europe Region" and "Latin America and the Caribbean Region" chapters.

3.14 Quarterly Mastercard Report (QMR)

Each Customer must complete and timely deliver to the Corporation the Quarterly Mastercard Report (QMR) in the manner and at such time as the Corporation requires.

3.14.1 Report Not Received

If the Corporation does not receive a Customer's properly completed QMR questionnaire when and how due, the Corporation may:

1. Impose on the Customer, after review of the Customer's last correctly submitted QMR questionnaire and assessment paid, an assessment equal to, or greater than, the Customer's assessment for such calendar quarter;
2. Impose on the Customer a noncompliance assessment;
3. If the Customer's actual payment based on the QMR questionnaire submitted by the Customer compared with the Corporation's estimate of payment due results in an underpayment by the Customer, collect the amount of the underpayment due and impose an interest penalty of the lower of two percent per month or the highest rate permitted by law, from the date the payment was first due through the date on which the additional amount due is paid;
4. If the Customer's actual payment based on the QMR questionnaire submitted by the Customer compared with the Corporation's estimate of payment due results in an overpayment by the Customer, return the amount of the overpayment, without interest or penalty thereon, as soon as practicable after the overpayment amount is identified and calculated; and
5. Collect the assessment amount and any penalty and interest due thereon from the Customer's settlement account.

3.14.2 Erroneous or Incomplete Report

If a Customer submits an erroneous or incomplete QMR, the Corporation may:

1. Impose on the Customer, after review of the Customer's last correctly submitted QMR and assessments paid thereon, an assessment equal to, or greater than, the Customer's last properly paid assessment for each calendar quarter for which it submitted an erroneous or incomplete QMR;
2. Impose on the Customer a noncompliance assessment;
3. If the Corporation's estimate of payment due results in an underpayment by the Customer, collect the amount of the underpayment due and impose an interest penalty of the lower of two percent per month or the highest rate permitted by law, from the date the payment was first due and payable through the date on which the additional amount due is paid;
4. If the Corporation's estimate of payment due results in an overpayment by the Customer, return the amount of the overpayment, without penalty or interest thereon, as soon as practicable after the overpayment amount is identified and calculated; and
5. Collect the assessment amount and any penalty and interest due thereon from the Customer's settlement account.

3.14.3 Overpayment Claim

After the Customer delivers a completed QMR to the Corporation, the Customer may submit a claim asserting an overpayment thereon.

The Corporation may review such claim if the claim is received by the Corporation no later than one calendar quarter after the date of the purported overpayment. If the Corporation substantiates the Customer's overpayment claim, the Corporation will return the amount of the overpayment to the Customer as soon as practicable, without interest or penalty thereon.

3.15 Cooperation

A Customer must fully cooperate with the Corporation and all other Customers in the resolution of Cardholder, Account Holder, and settlement disputes.

A Customer, to the best of its ability, must provide requested investigative assistance to any other Customer.

3.16 Issuer Reporting Requirement—EEA, Serbia, Gibraltar and United Kingdom

NOTE: Rules on this subject appear in the "Europe Region" chapter.

3.17 BINs

The Corporation may assign a Customer that engages in or is approved by the Corporation to engage in Activity one or more bank identification numbers (BINs).

The Corporation may assign BINs at its discretion from the following block ranges:

- Mastercard: 222100 to 272099 and 510000 to 559999
- Maestro: 639000 to 639099 and 670000 to 679999

Use of a BIN may not be sublicensed or re-assigned or otherwise transferred without the prior express written consent of the Corporation. A Principal or Association may permit a Sponsored Affiliate or a Sponsored Program Manager to use a Corporation Asset, provided that the Corporation receives all information and material required by Rule 3.2.

The Corporation may:

- Review a Customer's BIN usage for compliance with the Standards; and
- Retract the assignment of any BIN that has been assigned to a Customer.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

3.18 Recognized Currencies

The currencies recognized by the Corporation are listed in Chapter 2 of the *Quick Reference Booklet*.

Only currencies recognized by the Corporation may be:

- Loaded to a Card or Account; and
- Used to effect Transactions or PTA Transactions.

A Customer must convert any currency or other value not recognized by the Corporation, such as cryptocurrency, to a currency recognized by the Corporation before depositing any funds resulting from the conversion to a Card or Account or transferring any funds in any PTA Transactions. The conversion must take place in accordance with applicable laws and regulations.

3.18.1 Prior Consent of the Corporation

A Customer must not engage in Activity using a currency or other value not recognized by the Corporation, such as cryptocurrency, without the express prior written consent of the Corporation.

Examples of such Activity include, by way of example and not limitation:

- The funding of a Card with a currency recognized by the Corporation converted from a currency or other value not recognized by the Corporation;

- The funding of a MoneySend™ Payment Transaction with a currency recognized by the Corporation converted from a currency or other value not recognized by the Corporation; and
- The loading of a Digital Wallet which funds a Mastercard product with a currency recognized by the Corporation converted from a currency or other value not recognized by the Corporation.

The Corporation has the right to permit or not permit any proposed Activity. The Corporation may withdraw its permission at any time and without prior notice.

3.18.2 Communications and Marketing Materials

A Customer must not use or display any communication or marketing material that links a Card or Account or PTA Account to a currency or other value not recognized by the Corporation without the express prior written consent of the Corporation.

Chapter 4 Use of the Marks

This chapter contains Rules relating to the use of the Marks.

4.1 Right to Use the Marks

A right to use one or more of the Marks is granted to Customers and other Licensees only pursuant to the terms of a License with the Corporation.

Except as set forth in Rule 1.5, a Mark must not be used in any form or manner before the License is granted.

No additional interest in the Marks is granted with the grant of a right to use the Marks. A Licensee is responsible for all costs and liabilities resulting from or related to its use of a Mark or the Interchange System.

Except as set forth in Rule 1.9.2, each License is non-exclusive and non-transferable. The right to use a Mark may be sublicensed by a Licensee to any Sub-licensee only in accordance with the Standards or otherwise with the express written consent of the Corporation. A Customer or other Licensee that is permitted to sublicense the use of a Mark to a Sub-licensee must ensure, for so long as the sublicense is in effect, that the Mark is used by the Sub-licensee in accordance with the Standards and/or other additional conditions for such use required by the Corporation.

The right to use a Mark cannot be sublicensed or assigned, whether by sale, consolidation, merger, amalgamation, operation of law, or otherwise, without the prior written consent of the Corporation.

The Corporation makes no express or implied representations or warranties in connection with any Mark and the Corporation specifically disclaims all such representations and warranties.

4.1.1 Protection and Registration of the Marks

Protection of the Marks is vital to the Corporation, its Customers and other Licensees.

Any use of a Mark must not degrade, devalue, denigrate, or cause injury or damage to the Marks or the Corporation in any way.

By using any Mark, each Customer and other Licensee acknowledges that the Corporation is the exclusive owner and/or licensor of the Marks, and agrees not to contest or assist others, either directly or indirectly, in contesting the Corporation's sole ownership of the Marks, or otherwise take or fail to alert the Corporation of any action that would be inconsistent with that ownership. All use of any Mark will inure solely to the benefit of the Corporation.

No Customer or other Licensee or Sub-licensee or any of its affiliates may register, attempt to register or in any way make use of a Mark, or any mark or term the Corporation in its sole discretion deems to be derivative of, similar to, dilutive of or in any way related to a Mark on any Card, device, or other application associated with a payment service that the Corporation deems to be competitive with any Activity of the Corporation. Without limitation, the foregoing shall specifically apply to registration or use of any mark or term that incorporates, references, or otherwise could be confused or associated with any Mark currently or previously Licensed, sublicensed (to the extent sublicensing has been previously permitted), or used by a Customer, its Sub-licensees and permittees, and their respective successors or assignees (including, without limitation, by virtue of acquisition by merger or otherwise, bankruptcy or voluntary or

involuntary winding-up.). In particular, no use of a Mark may be made on or in connection with any card, device or other application associated with a payment service that the Corporation deems to be competitive with any Activity.

Without limitation, the foregoing shall apply to the registration or use of any mark or term that incorporates, references or otherwise could be confused or associated with a Mark currently or previously Licensed, sublicensed, or otherwise used by a Customer, the Customer's Sub-licensees and permittees, and their respective successors or assignees (including, without limitation, by means of acquisition by merger or otherwise, bankruptcy or voluntary or involuntary winding-up).

The Corporation reserves the right to determine, establish and control the nature and quality of the services rendered by its Customers under any mark the Corporation adopts.

In order to preserve the integrity of the Marks and prevent irreparable harm to the Corporation, each Customer agrees to cease using the Marks immediately upon written demand by the Corporation, and consent to the entry of an injunction against their continued use.

If a Customer is threatened with litigation, or is sued with regard to any matter relating to use of the Marks, and such other marks, the Customer must immediately notify the Corporation in writing. The Corporation, in its discretion, may then defend, settle, or consent to the entry of a judicial order, judgment or decree that would terminate any such litigation, or permit such Customer to do so.

NOTE: Modifications to this Rule appear in the "Europe Region" and "Additional U.S. Region and U.S. Territory Rules" chapters.

4.1.1.1 Registration of a Card Design

A Customer or other Licensee must not register with any trademark, copyright, patent or other intellectual property authority or attempt to register any Card design that includes a Mark or an EMVCo Mark.

4.1.2 Misuse of a Mark

A Customer or other Licensee must promptly notify the Corporation whenever the Customer or other Licensee learns of any misuse of any Mark or of any attempt to copy or infringe any of the Marks.

4.2 Requirements for Use of a Mark

The following requirements apply to the use of a Mark.

1. A Mark may be used only pursuant to a License. This provision applies, without limitation, to:
   a. Use of a Mark for advertising or promotional purposes;
   b. Placing an order for Card stock or for any other material bearing a Mark;
   c. Displaying a Mark;
   d. Issuing a Card;

e. Signing a Merchant to a Merchant Agreement; and
f. Distributing or affixing decals.

2. A Mark may only be used by a Customer or other Licensee to identify and promote Activity.
3. Any use of a Mark must comply with the terms of the License and the Standards, including all of the Corporation's reproduction, usage, and artwork Standards pertaining to such Marks.
4. The applicable Mark must be prominently displayed in all advertising, marketing, promotional, and collateral materials promoting a program or service offered by the Corporation. The inclusion of the Word Mark in the headline or title, or the prominent display of the Word Mark on the first page of the Solicitation satisfies this requirement. Each Solicitation must also include one or more of the following statements, as applicable to the program or service promoted (except small-size marketing communications):
   - "Mastercard and the circles design are registered trademarks of Mastercard International Incorporated."
   - "Maestro and the circles design are registered trademarks of Mastercard International Incorporated or its affiliates."
   - "Cirrus and the circles design are registered trademarks of Mastercard International Incorporated."

4.3 Review of Solicitations

The Corporation reserves the right to review samples and approve or refuse to approve use of a Solicitation.

Amended samples, if required as a result of this review, also must be forwarded to the Corporation for review.

4.4 Signage System

The Corporation's interlocking circles signage system is employed when one or more of the Corporation's brands is accepted at a Point of Interaction (POI).

The system requires the consecutive vertical or horizontal display of the Acceptance Marks in the following sequence—Mastercard, Maestro, Cirrus. Of the three brands, only the Marks of those brands that are accepted at a particular POI location may be displayed there.

A Customer must comply with all of the following requirements for display of the Marks:

1. The Marks must be displayed as set forth in the Standards, including those posted on the Mastercard Brand Center website at brand.mastercard.com
2. The Marks must not be separated by any other acceptance marks or Access Marks displayed on the same Terminal.
3. The Marks must not be placed on or near or otherwise be used to identify any acceptance device that does not accept Cards.

4. Signage must not be displayed in a false, deceptive, or misleading manner.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

4.4.1 Signage at a Merchant Location

The display of the Acceptance Marks at a Merchant location must comply with Rule 5.10.1.

With respect to a Maestro Merchant location, the following applies.

1. The Corporation may permit or prohibit the display of the logo of a Competing EFT POS Network at POS Terminals displaying the Maestro Acceptance Mark.
2. On any new or replacement signage incorporating the marks of a Competing EFT POS Networks or any other international, regional, or bilateral acceptance marks, the Maestro Acceptance Mark must be afforded at least equal prominence and be at least as large.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

4.4.2 ATM Terminal Signage

The Mastercard, Maestro, and Cirrus Marks must be displayed on an ATM Terminal.

On new or replacement signage incorporating any Competing ATM Network marks, the Acceptance Marks must be afforded at least equal prominence and be at least as large as a Competing ATM Network mark. On an ATM Terminal displaying an Access Mark, the Acceptance Marks must be afforded similar prominence to any Access Mark displayed (characteristics to consider for similar prominence include size, frequency, color treatment, and co-location within the same field of vision).

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

4.5 Use of the Interlocking Circles Device

The Corporation's interlocking circles devices, each of which incorporates a Word Mark, must be reproduced as set forth in the Mastercard Brand Center website at brand.mastercard.com and in the *Card Design Standards*.

4.5.1 Use or Registration of Similar Logos, Designs, and Names

A Customer, Licensee, or Sub-licensee may not use or seek to register any logo, design, or decorative element that includes two or more interlocking, adjoining, or adjacent circles, spheres, globes, or similar shapes that, in the opinion of the Corporation, may be likely to cause confusion with, or create a false association, connection or affiliation with, or dilute the distinctiveness of any of the Corporation's interlocking circles devices.

4.6 Use of Multiple Marks

When two or more Marks that use the interlocking circles device are displayed together, they must have visual parity with one another.

When promoting any Mark with another acceptance mark in any media to denote acceptance, no other acceptance mark, symbol or logo may be or appear to be larger or more important than or more welcomed than the Mark. To maintain visual parity, an Acceptance Mark must be at least as prominent as, and appear in at least the same frequency, size, and color treatment as, any other acceptance mark displayed. To maintain parity within written text, a Word Mark must be at least as prominent as, and appear at least as frequently as, any other acceptance mark mentioned.

NOTE: Refer to Rule 5.12 of "Additional U.S. Region and U.S. Territory Rules" for modifications on the use of the Mastercard Brand Mark.

4.7 Particular Uses of a Mark

A Customer must comply with all of the following Standards and the Standards set forth in the Mastercard Brand Center website at brand.mastercard.com regarding particular uses of a Mark.

4.7.1 Generic Use

A generic term, such as "bank card" or "payment card," does not function as a Mark. Use of a Mark in a manner that would tend to genericize that Mark or otherwise result in the loss of trademark rights is prohibited.

4.7.2 Use of Modifiers

A Customer is permitted to use its name or a geographical designation in conjunction with a Word Mark, such as "California Mastercard card program" or "First Issuer Maestro Department."

The Corporation may prohibit the use of a modifier that it determines will impair the distinctiveness of any Mark or create any likelihood of confusion or reflect poorly on the Corporation.

4.7.3 Use on Stationery

A Licensee is permitted to use a Mark on print or electronic stationery, letterhead, envelopes, and the like for the purpose of identifying its Program or service.

If a Word Mark is used, the Licensee's name must appear in close proximity to it, such as "Superior National Bank Cirrus® Department."

4.7.4 Use on Non-Licensed Products or Services

A Mark may not be used in a manner likely to create an impression that any product or service offered by the Licensee, Sub-licensee, or Merchant is sponsored, produced, offered, approved, sold by, or otherwise affiliated with the Corporation.

Each Licensee must ensure that each of its Sub-licensees, partners, Merchants, and other Program participants does not apply a Mark to any product or service not expressly permitted by a License.

4.7.5 Use or Registration of "Master," "Maestro," and "Cirrus" Terminology

Except as expressly permitted in writing by the Corporation, the words "Master," "Maestro," and "Cirrus" may not be used or registered as part of a trademark, service mark, corporate name, business name, or Program name, whether preceding, following or linked together as one word, or with a hyphen or slash, or in connection with any financial or bank-related products or services.

4.7.6 Use of a Word Mark in a Corporate, Business or Domain Name

A Word Mark may not be used as part of a legal, corporate, or business name, such as "Mastercard Center, Inc."

No Internet domain name may be registered that includes the words "Mastercard," "Maestro," or "Cirrus," except as expressly permitted in writing by the Corporation.

A Customer seeking to include the words "Mastercard," "Maestro," or "Cirrus" in an Internet domain name must submit a request with a detailed explanation and the circles design and an executed Mastercard Domain Name License Agreement (available on **Mastercard Connect** > **Support** > **Forms**) to Service_Provider@mastercard.com. If the Corporation agrees to permit such use by a Customer, the Corporation will execute such Mastercard Domain Name License Agreement.

4.7.7 Use of a Word Mark in Text

A Word Mark must be used as an adjective (as in "your Maestro® card") in the first or most prominent use subsequent to any use in the title, headline, signature, or cover page of an offering, unless:

1. The word "Mastercard," "Maestro," or "Cirrus" is used as part of a Customer's Program name (as in "Customer/Program name Mastercard"); or
2. Otherwise expressly approved in writing by the Corporation.

The word "Mastercard," "Maestro" and "Cirrus" must not be modified in any way and may only be in all uppercase letters if the font style of the user interface or communication also appears in all uppercase letters.

Use of the word "Mastercard," "Maestro," or "Cirrus" as a verb ("Mastercard your gifts"), in plural ("Mastercards") or in possessive form ("Mastercard's") is prohibited. Use of the word "Mastercard," "Maestro," or "Cirrus" as a verb, in plural or in possessive form must be

accompanied by a reference to card or account ("Mastercard card," "Mastercard cards" or "Mastercard card's").

4.7.8 Program Names

Each Program name, Solicitation, and service must be referred to by the full, legal name of the applicable brand and include the appropriate registration notice.

4.7.9 Use on Cards

Standards governing the use of Marks on Cards, including but not limited to Multi-Account Chip Cards and other Cards displaying co-residing Marks, are set forth in the *Card Design Standards*, available on Mastercard Connect™, which are incorporated into these Rules by reference.

A Customer must also comply with all of the following Standards regarding the particular uses of a Mark.

4.8 Use of Marks on Maestro and Cirrus Cards

A Customer that permits any of its debit cards access to the Interchange System must begin issuing debit cards in compliance with the Standards for Maestro and/or Cirrus Cards, as applicable, no later than nine months after the date that any of its debit cards first had access to the Interchange System.

The Portfolios must be in full compliance with the Standards no later than 36 months after the date that any of its debit cards first had access to the Interchange System.

The Maestro Brand Marks may not be placed on any debit card that is not eligible to be a Maestro Card or on any credit card.

A Customer must not place any Competing EFT POS Network debit marks on a Maestro Card.

A Visa card issued by a Customer may display only the Cirrus Word Mark, which must be a minimum of one-half (1/2) inch across measured horizontally, not including the required registration mark.

NOTE: Modifications to this Rule appear in the "Europe Region," "Latin America and the Caribbean Region," and "Additional U.S. Region and U.S. Territory Rules" chapters.

4.9 Use of Marks on Mastercard Cards

No acceptance mark may appear on a Mastercard Card except as set forth in the Standards, including the *Card Design Standards* manual and other Card design specifications.

Except as expressly permitted by the Corporation, none of the following marks or any similar or related mark, or any mark owned by or affiliated with one of these entities, may appear on a Card.

1. American Express

2. JCB
3. Diners Club
4. Discover
5. Visa
6. Any other name, logo, or mark identifying or in any way associated with a payment service that the Corporation deems to be competitive with any Mastercard product or Program.

Any such competitor's credit or debit POI mark, logo, or name, regardless of whether registered, may not appear on a Card, nor may a payment application of any such competitor reside on the magnetic stripe or chip of a Card. The appearance of the PLUS word mark on the back of the Card is permitted where there is an effective PLUS agreement with the Issuer.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," and "Additional U.S. Region and U.S. Territory Rules" chapters.

4.10 Use of a Card Design in Merchant Advertising and Signage

A Merchant is prohibited from using a Mastercard or Maestro Card design to indicate acceptance in Merchant advertising or other signage, other than signage for a Co-Brand Program in which the Merchant is a Co-Brand Partner.

A Merchant may display an Issuer-specific Mastercard or Maestro Card design in Merchant advertising and any other signage that is not used to signify acceptance.

4.11 Use of a Card Design in Issuer Advertising and Marketing Material

An Issuer is permitted to depict a Mastercard, Maestro, or Cirrus Card face for an advertising or marketing purpose, subject to the following requirements.

1. The proportions of the Card face design, including typestyle and relative positions of the legends, may not be altered or distorted.
2. The Mastercard Brand Mark, Mastercard Symbol, or Mastercard Premium Brand Mark must be completely visible on at least one Card face design depicted in the materials.
3. If included, the Account information (for example, the Primary Account Number (PAN effective date and/or expiration date, and the cardholder name) and all Card face design requirements must be in accordance with the requirements set forth in the *Card Design Standards*. If included, the first six digits of the Account number must be either a BIN assigned to the Issuer by the Corporation or the unassigned BIN 541275 or 222100, which the Corporation has set aside for Issuer use in advertising and marketing Card face designs.
4. When a Cardholder name is present on the card image, the Issuer must use the name M. Molina in the Latin America and the Caribbean Region or the name Lee M. Cardholder or John M. Cardholder in all other Regions.

4.12 Use of the Mastercard Card Design in Cardholder Statement Enclosures

The Mastercard Card face design must be displayed on statement enclosures used to offer products or services to Cardholders through the use of a Customer's Mastercard Card.

The Mastercard Brand Mark or Mastercard Symbol may be used in lieu of the Card face design if the Customer's name is displayed on the statement enclosure.

4.13 Use of the Brand Marks on Other Cards

A Brand Mark must not be used on a promotional card or other card without the prior written consent of the Corporation.

4.14 Use of EMVCo® Trademarks

The Corporation grants to Customer or other Licensee under the Corporation's licenses with EMVCo, LLC ("EMVCo") a right to use one or more of the QR, Contactless and Secure Remote Commerce logos, designations, symbols, and marks that EMVCo owns, manages, licenses, or otherwise Controls (collectively, the "EMVCo Marks"). This right is subject to the terms and conditions set forth in the Standards, including those posted on the Mastercard Brand Center website at brand.mastercard.com and the EMVCo specifications available from EMVCo, including from the Internet website of EMVCo (currently located at www.emvco.com, as such website address may change from time to time) (the "EMVCo Specifications").

No additional interest in the EMVCo Marks is granted with the grant of a right to use the EMVCo Marks. A Customer or other Licensee is responsible for all costs and liabilities resulting from or related to its use of an EMVCo Mark.

This right to use the EMVCo Marks is non-exclusive and non-transferable. The right to use an EMVCo Mark may be sublicensed by a Licensee to a permitted Sub-licensee only in accordance with the Standards and the EMVCo Specifications or otherwise with the express written consent of the Corporation or EMVCo. A Customer or other Licensee that is permitted to sublicense the use of an EMVCo Mark to a permitted Sub-licensee must ensure, for so long as the sublicense is in effect, that the EMVCo Mark is used by the Sub-licensee in accordance with the Standards, the EMVCo Specifications and/or other additional conditions for such use required by the Corporation or EMVCo. Except as expressly permitted by this paragraph, the right to use an EMVCo Mark cannot be sublicensed or assigned, whether by sale, consolidation, merger, amalgamation, operation of law, or otherwise, without the prior written consent of the Corporation.

The Corporation makes no express or implied representations or warranties in connection with any EMVCo Mark and the Corporation specifically disclaims all such representations and warranties.

Chapter 5 Acquiring Activity

This chapter contains Rules relating to Merchant and ATM Owner Agreements, Acquirer and Merchant obligations, and Card acceptance requirements.

5.1 The Merchant and ATM Owner Agreements

Each Customer in its capacity as an Acquirer must directly enter into a written Merchant Agreement with each retailer or other person, firm, or corporation selling goods or services (herein, a "seller") and must directly enter into a written ATM Owner Agreement with each ATM owner from which it acquires Transactions, whether such Transactions are submitted to the Customer directly by the seller or ATM owner or through a Service Provider acting for or on behalf of such Customer. A Merchant Agreement is not required in connection with Transactions acquired by an Acquirer from its registered Payment Facilitator, when submitted pursuant to a Submerchant Agreement between the Payment Facilitator and a seller.

The Acquirer must acquire all valid Transactions submitted to it from a Merchant in accordance with the Merchant Agreement, and all valid ATM Transactions in accordance with the ATM Owner Agreement. An Acquirer must not submit for processing through the Interchange System any Transaction resulting from the acceptance of a Card by an entity or person except pursuant to a Merchant Agreement or ATM Owner Agreement then in effect between the Acquirer and the entity or person.

Each Merchant Agreement and each ATM Owner Agreement must reflect the Acquirer's primary responsibility for the Merchant or ATM owner relationship and the establishment of all management and operating policies relating to its acquiring Programs, and must otherwise comply with the Standards. A Merchant Agreement or ATM Owner Agreement must not include any provision that limits, or attempts to limit, the Acquirer's responsibility for such Programs.

An Acquirer in violation of this Rule may be assessed up to USD 2,500 per day with respect to each entity or person on whose behalf the Acquirer submits Transactions into interchange with no Merchant Agreement being in effect between the Acquirer and the entity or person, retroactive to the first day of such noncompliant practice.

5.1.1 Verify Bona Fide Business Operation; Government Controlled Merchants

Before entering into, extending, or renewing a Merchant Agreement, an Acquirer must inquire and verify whether that Merchant from which it intends to acquire Transactions is a Government Controlled Merchant.

An Acquirer must not onboard, or maintain a Merchant-related relationship with, any Government Controlled Merchant whose home country government is subject to sanctions laws and regulations enacted by United States sanctions authorities (including, OFAC and the United States Department of State), as well as applicable local sanctions regulations where the Activity is taking place.

Before entering into, extending, or renewing a Merchant Agreement or ATM Owner Agreement, an Acquirer must verify that the Merchant or ATM owner from which it intends to acquire Transactions is a bona fide business, has sufficient safeguards in place to protect Account data from unauthorized disclosure or use, and complies with applicable laws, and that each POS Transaction will reflect bona fide business between the Merchant or Submerchant and a Cardholder. Procedures for verifying that a Merchant or ATM owner is a bona fide business are set forth in Chapter 7 of the *Security Rules and Procedures* manual.

5.1.2 Required Merchant Agreement Terms

Each Merchant Agreement must contain the substance of each of the Standards set forth in Rules 5.5 through 5.14, and any other Standards applicable to the nature and manner of the Merchant's business.

The failure to include the substance of any one or more of such Standards in the Merchant Agreement or the grant of a variance by the Corporation with respect to any one or more such Standards does not relieve an Acquirer from responsibility for chargebacks or compliance.

Each Merchant Agreement may contain only such terms agreed to by the Acquirer and the Merchant, provided that no such term conflicts with any Standard. The Merchant Agreement must also provide that the Merchant's use or display of any Mark will terminate effective with the termination of the Merchant Agreement or upon notification by the Corporation to discontinue such use or display.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "Middle East/ Africa Region," and "United States Region" chapters.

5.1.2.1 Gambling Merchants

Each Merchant Agreement with a Merchant proposing to engage in gambling Transactions must incorporate the following terms.

1. If the Merchant proposes to engage in Internet gambling Transactions, the Merchant must post a notice on its websites (in a position such that the notice will be displayed before Account information is requested, such as a click-through notice) stating that assertions have been made that Internet gambling may not be lawful in some jurisdictions, including the United States, and suggesting that the Cardholder check whether Internet gambling is lawful under applicable law.
2. A Merchant must not sell chips or other value that can be used, directly or indirectly, to gamble at locations other than those that the Merchant wholly owns.
3. A Merchant must not use a refund Transaction to credit winnings or value usable for gambling or gaming to a Mastercard or Maestro Account. Refer to Chapter 6 of the *Transaction Processing Rules* manual and the *Mastercard Gaming and Gambling Payments Program Standards* for Standards applicable to use of the Gaming Payment Transaction to transfer winnings or value usable for gambling or gaming to a Mastercard or Maestro Account.
   For the avoidance of doubt, a refund Transaction conducted to return funds not used for gambling or gaming (for example, a Cardholder changed his or her mind prior to gambling or gaming) or in response to a Cardholder claim of fraud is not considered the crediting of winnings or value usable for gambling or gaming to a Mastercard or Maestro Account.
4. All non–face-to-face gambling Transactions effected with a Mastercard Card or Account must include at least one of the following in the Authorization Request/0100 message:
   a. The CVC 2 value in DE 48 (Additional Data—Private Use), subelement 92 (CVC 2);
   b. A valid Accountholder Authentication Value (AAV) in DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) resulting from an EMV 3DS authentication; or
   c. In the case of a recurring payment Transaction, Identity Check Insights (previously known as Data Only).

A non-face-to-face gambling Transaction is identified with any of the following MCCs:

- MCC 7800 (Government Owned Lottery [U.S. Region Only])
- MCC 7801 (Internet Gambling [U.S. Region Only])
- MCC 7802 (Government Licensed Horse/Dog Racing [U.S. Region Only])
- MCC 7995 (Gambling Transactions)
- MCC 9406 (Government-owned Lottery [Specific Countries]).

Refer to the *Mastercard Identity Check Program Guide* for information about Identity Check Insights and EMV 3DS authentication using Mastercard Identity Check.

NOTE: Modifications to this Rule appear in the "Canada Region" and "United States Region" chapters.

5.1.3 Required ATM Owner Agreement Terms

The ATM Owner Agreement must, in substance, include all of the following terms.

1. The ATM owner received, understands, and agrees to comply with all Standards that apply to the nature and manner of the ATM owner's business as that business relates to the ownership and/or deployment of an ATM.
2. On an ongoing basis, and in no event less than quarterly, the ATM owner is promptly to provide the Acquirer with all information for each of its ATM locations as required by the Corporation to maintain its Location Administration Tool (LAT), including but not limited to each ATM location name, address, and Terminal ID.
3. In the event of any inconsistency between any provision of the ATM Owner Agreement and the Standards, the Standards shall govern.
4. The ATM Owner Agreement automatically terminates if the Acquirer ceases to be a Customer for any reason. The Corporation retains the right to require that the Acquirer terminate the ATM Owner Agreement if the Corporation determines that any ATM owner appears not to be qualified for any reason.
5. The ATM owner acknowledges that the Corporation is the sole and exclusive owner of the Marks and agrees that the ATM owner will not contest the ownership of the Marks for any reason whatsoever. The Corporation may at any time, immediately and without advance notice, prohibit the ATM owner from using any of the Marks for any reason.
6. The ATM owner acknowledges and agrees that the Corporation has the right to enforce any provision of the Standards and to prohibit any ATM owner conduct that may injure or may create a risk of injury to the Corporation, including injury to reputation, or that may adversely affect the integrity of the Corporation's core payment systems, information, or both. The ATM owner must agree not to take any action that might interfere with, or prevent exercise of, this right by the Corporation.

5.1.4 Maintaining Information

The Acquirer must maintain, on an ongoing basis:

1. For each Merchant participating in the Acquirer's Program, the Merchant's name and address and a signed, unexpired Merchant Agreement; and

2. For each ATM owner participating in the Acquirer's Program, a signed, unexpired ATM Owner Agreement and all of the following information:
   a. The complete name and address of the ATM owner (or principals of the business if the ATM owner is a corporation, partnership, or limited liability company).
   b. The complete address of the ATM Terminal location, if different from that of the ATM owner.
   c. The ATM owner's legal status (for example, corporation, partnership, sole proprietor, non-profit, other), and the applicable Federal Taxpayer Identification Number (TIN), Federal Employer Identification Number (FEIN) or Social Security Number (SSN), or other equivalent government registration identifiers appropriate to the ATM owner's country of operation.
   d. The legal name, and if applicable the "Doing Business As" (DBA) name, of the ATM Terminal location.
   e. The complete name and address of any Third Party Processor (TPP) performing services for, or otherwise associated with, the ATM owner.
   f. The complete name and address of any entity, other than the ATM owner, that receives revenue as a result of the use, lease, placement, and/or maintenance of the ATM Terminal.
3. The supplier, manufacturer, and model of each of its ATM Terminals and Bank Branch Terminals.
4. For each Government Controlled Merchant, must identify the goods and services that the Government Controlled Merchant provides.

5.1.4.1 Location Administration Tool (LAT) Updates

The Acquirer must provide current and accurate information regarding its ATM Terminals and Bank Branch Terminals by means of quarterly updates to the Location Administration Tool (LAT) on Mastercard Connect™.

5.2 Merchant and Submerchant Compliance with the Standards

The Acquirer is responsible for ensuring that each of its Merchants and Submerchants complies with the Standards, and the Acquirer is itself responsible to the Corporation and to other Customers for any Merchant's or Submerchant's failure to do so.

To the extent a Merchant or Submerchant utilizes the service of a person or entity for a purpose arising from or related to Activity, the Acquirer is responsible for ensuring that each such person or entity complies with the Standards, and the Acquirer itself is responsible to the Corporation and to other Customers for any such person's or entity's failure to do so.

The Acquirer must not support any Merchant or Submerchant action having a purpose or effect of evading detection by the Corporation's fraud monitoring and other compliance thresholds set forth in the Standards, including but not limited to "load balancing" (that is, the distribution of Transactions between or among Merchant ID numbers in order to avoid minimum thresholds).

The Acquirer must take such actions as may be necessary or appropriate to ensure a Merchant's or Submerchant's ongoing compliance with the Standards by monitoring, on an ongoing basis,

the Activity and use of the Marks of each of its Merchants. Minimum Merchant monitoring Standards are set forth in Chapters 6 and 7 of the *Security Rules and Procedures* manual.

Failure by a Merchant, Submerchant, or Acquirer to comply with any Standard may result in chargebacks, an assessment to the Acquirer, and/or other disciplinary action.

5.2.1 Noncompliance Assessments

If the Corporation becomes aware of a Merchant's noncompliance with any Standard, the Corporation may notify the Acquirer and may assess and/or otherwise discipline the Acquirer for such noncompliance, and the Acquirer must promptly cause the Merchant to discontinue the noncompliant practice.

A notification by the Corporation with respect to any one location of a Merchant requires the Acquirer to ensure that the Merchant is in compliance with the Standards at all locations of the Merchant that are subject to the Merchant Agreements.

As set forth in Rule 2.1.6, a Customer may request that the Chief Franchise Officer of the Corporation review an assessment for a Merchant's noncompliance with a Standard.

5.3 Deferred Delivery Merchant

A deferred delivery merchant ("DDM") is a Merchant whose primary business accepts advanced payments from Cardholders on a high Volume of Transactions for goods and/or services, but usually has an extended time frame for delivery of such goods and/or services.

Regular Monitoring of DDMs

An Acquirer acquiring Transactions for a DDM must regularly review and monitor the DDM's Transaction Volumes to ensure that the Acquirer is sufficiently managing any credit, financial and other risks associated with the DDM.

Information and Consent

Any Acquirer that is interested in acquiring Transactions for a new DDM under any of the following MCCs must seek and obtain the Corporation's written consent before acquiring Transactions for such DDM, by sending a completed Deferred Delivery Merchant form (Form 1358) in an email to DDM_Enquiries@mastercard.com with subject: "CRM Request for Consent to DDM Acquiring– [INSERT REGION & COUNTRY]". Form 1358 is available on **Mastercard Connect** > **Support** > **Forms**.

NOTE: Refer to Appendix A for the list of Countries by Region.

- Airlines and Air Carrier (MCCs 3000 through 3350, 4511)
- Car Rental Agencies (MCCs 3351 through 3500, 7512)
- Cruise Lines (MCC 4411)
- Direct Marketing: Travel-Related Arrangement Services (MCC 5962)

- Lodging: Hotels, Motels, Resorts (3501 through 3999, 7011)
- Motor Home and Recreational Vehicle Rental (MCC 7519)
- Real Estate Agents and Managers: Rentals (MCC 6513)
- Theatrical Producers (excluding Motion Picture) Ticket Agencies (MCC 7922)
- Timeshares (MCC 7012)
- Travel Agencies and Tour Operators (MCCs 4722)

Conditional Consent

In its consent of an Acquirer's request to acquire Transactions for a new DDM, the Corporation may establish conditions, which the Acquirer must follow prior to submitting any DDM Transaction for processing through the Interchange System.

Such conditions may include implementation of enhanced due diligence on a DDM and risk management controls such as those described in Rule 1.4. An Acquirer acquiring Transactions for a DDM must regularly review and monitor the DDM's Transaction Volumes to ensure that the Activity continues to meet any conditions established by the Corporation. In the event of any increase in Acquirer's DDM Transaction Volume) or change to any other conditions placed on the Acquirer by the Corporation, the Acquirer must immediately notify the Corporation of such changes by sending a completed Deferred Delivery Merchant form (Form 1358) in an email to DDM_Enquiries@mastercard.com with subject: "CRM Notice of DDM acquiring request – [INSERT REGION & COUNTRY]". Form 1358 is available on **Mastercard Connect** > **Support** > **Forms**.

NOTE: Refer to Appendix A for the list of Countries by Region.

Request for DDM Information

The Corporation reserves the right to request that an Acquirer complete Form 1358 for any DDM for which the Acquirer acquires Transactions.

Upon request from the Corporation, an Acquirer must provide the information contained in the Deferred Delivery Merchant form (Form 1358), and any other information requested by the Corporation, for the specified DDM, within five business days. Form 1358 is available on **Mastercard Connect** > **Support** > **Forms**.

Based on the Corporation's review and assessment that an Acquirer's DDM Transaction Volume presents risk to the Corporation, the Corporation, in its sole discretion, has the right to impose conditions or restrictions on such Acquirer with respect to its DDM Transactions.

5.4 Acquirer Obligations to Merchants

An Acquirer must fulfill all of the obligations set forth in this Rule 5.4 with respect to each of its Merchants.

5.4.1 Payment for Transactions

The Acquirer must pay the Merchant the amount (either gross or net of Merchant discount or setoff) of all Transactions that the Acquirer acquires from the Merchant in accordance with the Merchant Agreement and the Standards.

This obligation is not discharged with regard to a Transaction until the Merchant receives payment from the Acquirer that acquired the Transaction, notwithstanding any Acquirer payment arrangement, including any such arrangement between an Affiliate and its Sponsor. A Merchant Agreement may provide for an Acquirer to withhold amounts for chargeback reserves or similar purposes in accordance with the Standards.

5.4.2 Supplying Materials

The Acquirer must regularly ensure the Merchant is provided with all materials necessary to conduct POS Transactions in accordance with the Standards and to signify Card acceptance.

These materials may include POS Terminals, PIN pads, Card acceptance decals, signage, and the like.

NOTE: A modification to this Rule appears in the "Asia/Pacific Region" chapter.

5.4.3 Provide Information

NOTE: Rules on this subject appear in the "Europe Region" and "United States Region" chapters.

5.4.4 Merchant Deposit Account—Canada Region Only

NOTE: A Rule on this subject appears in the "Canada Region" chapter.

5.5 Merchant Location

Except as otherwise provided in the Standards, a Merchant may accept Cards only at locations that are within the Acquirer's Area of Use.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

A Merchant's location is at an address in the country where the Merchant conducts the business described in the Merchant application and governed by the Merchant Agreement.

Merchant Location for Card-Present Transactions

The country of a Merchant proposing to engage in Card-present Transactions is the country in which the Transaction takes place. Refer to Rule 5.8.5 regarding Transactions occurring at a POS Terminal with no fixed location.

Merchant Location for Card-Not-Present Transactions

The country of a Merchant proposing to engage in Card-not-present Transactions is the country in which the Acquirer must certify that, and by entering into a Merchant Agreement with the Merchant does certify with respect to that Merchant that all of the following criteria are satisfied:

1. **The Merchant conducts business locally.**
   The Merchant conducts business activity and operations directly related to Transactions in the country. By way of example and not limitation, a post office box address, the location at which a server is stored, the address of a warehouse having no business-related functions, the Uniform Resource Locator (URL) of a website, or address of the Merchant's law firm, vendor, or agent does not satisfy this requirement.
2. **The Merchant holds permits to operate locally.**
   The Merchant holds all necessary permits required under applicable law or regulation to conduct its business activity and operations in the country as a domestic entity.
3. **The Merchant complies with local tax laws and regulations.**
   The Merchant has represented to the Acquirer that it pays or will pay income tax on profits attributable to Transactions in the country (to the extent that taxes apply) and is registered to collect (regardless of whether actually required to collect) indirect taxes, including but not limited to value-added tax (VAT), goods and services tax (GST), Programa de Integração Social (PIS), Contribuição para o Financiamento da Seguridade Social (COFINS), sales tax, and any similar tax, in the country.
4. **The Merchant is subject to local consumer laws and courts.**
   Except as otherwise may be permitted by applicable local consumer law, the Transaction terms and conditions established by the Merchant state that the Merchant, as the contractual counterparty to the consumer, is subject to the laws and courts of the country.

5.5.1 Disclosure of Merchant Name and Location

An Acquirer must ensure that each of its Merchants prominently and clearly discloses to the Cardholder at all points of interaction:

1. The name of the Merchant, so that the Cardholder can easily distinguish the Merchant from any other party, such as a supplier of products or services to the Merchant; and
2. The location (physical address) of the Merchant to enable the Cardholder to easily determine, among other things, whether the Transaction will be a Domestic Transaction or a Cross-border Transaction. The Merchant location must be disclosed before the Cardholder is prompted to provide Card information.

The Merchant name and country location, as disclosed to the Cardholder at the POI and on Transaction receipts, must be the same as what is provided in authorization and clearing Transaction messages.

NOTE: An additional Rule on this subject appears in the "Europe Region" chapter.

5.5.2 Merchant Location Compliance and Certification

The Corporation reserves the right to request that the Acquirer provide to the Corporation a written certification statement signed by one or more of the Merchant's duly authorized senior executives or officers attesting:

- That the country specified to the Acquirer as the Merchant's location satisfies all of the criteria set forth in Rule 5.5; and
- That the address disclosed to Cardholders and appearing in Transaction messages is a location in the specified country, and is an address from which the Merchant is conducting the business activity and operations governed by the Merchant Agreement.

The Corporation, at its sole discretion, has the right to make a final determination of a Merchant's location that is binding upon the parties to the Merchant Agreement.

Any disagreement between Customers regarding a Merchant's location may be referred to the Corporation for final resolution.

5.6 Submerchant Location

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

Except as otherwise provided in the Standards, a Submerchant may accept Cards only at locations that are within the Acquirer's Area of Use.

A Submerchant's location is at an address in the country where the Submerchant conducts the business described in the Submerchant application and governed by the Submerchant Agreement. The Acquirer is responsible for verifying that the Submerchant address set forth in the Submerchant Agreement and any address disclosed to Cardholders or appearing in Transaction messages is a location from which the Submerchant is conducting such business, or the Acquirer may permit the Payment Facilitator to manage this obligation on its behalf.

In determining the country of the Submerchant, the Acquirer must certify that the Submerchant satisfies all of the criteria for Card-present Transactions or Card-not-present Transactions or both, as applicable, set forth in Rule 5.5. The Acquirer may permit the Payment Facilitator to manage this obligation on its behalf.

5.6.1 Disclosure of Submerchant Name and Location

An Acquirer must ensure that each of its Payment Facilitators' Submerchants prominently and clearly discloses to the Cardholder at all points of interaction:

1. The name of the Submerchant, so that the Cardholder can easily distinguish the Submerchant from any other party, such as a supplier of products or services to the Submerchant; and

2. The country location of the Submerchant to enable the Cardholder to easily determine, among other things, whether the Transaction will be a Domestic Transaction or a Cross-border Transaction. The Submerchant location must be disclosed before the Cardholder is prompted to provide Card information.

The Submerchant name and country location, as disclosed to the Cardholder at the POI and on Transaction receipts, must be the same as what is provided in authorization and clearing Transaction messages.

NOTE: An additional Rule on this subject appears in the "Europe Region" chapter.

5.6.2 Submerchant Location Compliance and Certification

The Corporation reserves the right to request that the Acquirer provide to the Corporation a written certification statement signed by one or more of the Submerchant's duly authorized senior executives or officers attesting:

- That the country specified to the Acquirer or the Acquirer's Payment Facilitator as the Submerchant's location satisfies all of the criteria set forth in Rule 5.5; and
- That the address disclosed to Cardholders and appearing in Transaction messages is a location in the specified country, and is an address from which the Submerchant is conducting the business activity and operations governed by the Submerchant Agreement.

The Corporation, at its sole discretion, has the right to make a final determination of a Submerchant's location that is binding upon the parties to the Submerchant Agreement and the Acquirer.

Any disagreement between Customers regarding a Submerchant's location may be referred to the Corporation for final resolution.

5.7 Responsibility for Transactions

Each Merchant and Submerchant must ensure that the Cardholder is easily able to understand that the Merchant or Submerchant is responsible for the Transaction, including delivery of the goods (whether physical or digital) or provision of the services that are the subject of the Transaction, and for customer service and dispute resolution, all in accordance with the terms applicable to the Transaction.

5.8 Transaction Message Data

An Acquirer must ensure that each of its Merchants and Terminals complies with the Transaction message data requirements set forth in this Rule.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

5.8.1 Card Acceptor Business Code (MCC) Information

The Acquirer must ensure that each Merchant and Submerchant is identified in authorization and clearing Transaction messages with the Card acceptor business code (MCC) that reflects the primary business of the Merchant or Submerchant.

Any Transaction that includes the sale of products or services properly identified with one of the following MCCs must be identified with such MCC:

- Gambling Transactions (MCCs 7800, 7801, 7802, 7995, and 9406)
- Funding Transactions (MCCs 4829, 6538, and 6540)
- Quasi-cash Transactions (MCCs 6050 and 6051)

Transactions for the sale of non-fungible tokens (NFTs) may be identified with the MCC that best describes either the Merchant's primary business or the type of product or service being represented in digitized format (for example, MCC 7929 [Bands, Orchestras, and Miscellaneous Entertainers] for NFTs representing unique tickets to music concerts or MCC 5815 [Digital Goods: Audiovisual Media Including Books, Movies, and Music] for NFTs representing unique digital recordings of music concerts).

Transactions for the online sale of prepaid gift Cards must be identified as Funding Transactions (using MCC 6540) if such sales are the Merchant's primary business. All other sales of prepaid gift Cards may be identified with the MCC that best describes the Merchant's primary business

For MCC descriptions, refer to Chapter 3 of the *Quick Reference Booklet*.

The Corporation shall have the ultimate authority to dictate the appropriate MCC if any dispute shall arise.

NOTE: A modification to this Rule appears in the "Canada Region" and "United States Region" chapters.

5.8.2 Card Acceptor Address Information

The Acquirer must transmit the generally accepted location, city, and country of the Terminal or website in DE 43, substantially the same as it appears on any Transaction receipt provided.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

5.8.3 Submerchant Name Information

The Acquirer must ensure that a Transaction conducted by a Submerchant includes the names of both the Payment Facilitator and the Submerchant in DE 43 (Card Acceptor Name/ Location), subfield 1 (Card Acceptor Name). The Payment Facilitator name, in full or in abbreviated form, must be followed by "*" and the Submerchant name.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

5.8.4 ATM Terminal Information

The Acquirer of an ATM Transaction must transmit the ATM owner name and ATM location address, substantially the same as it appears on any Transaction receipt provided, in DE 43 (Card Acceptor Name/Location) and the unique ATM Terminal identification information in DE 41 (Card Acceptor Terminal ID) of each Transaction message.

An Acquirer and any Service Provider performing ATM Transaction processing services must also identify itself using a unique number, which is assigned by the Interchange System.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

5.8.5 Transactions at Terminals with No Fixed Location

A Transaction arising from a Terminal with no fixed location (for example, aboard a train or ship) may be deemed to take place in the country where the Merchant operating a POS Terminal or the Acquirer of an ATM Terminal or Bank Branch Terminal is headquartered or where the Transaction is processed.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

5.8.6 Enablement of QR-based Payments

NOTE: A Rule on this subject appears in the "Latin America and the Caribbean Region" chapter.

5.9 Transaction Currency Information

Prior to acquiring Transactions on which POI currency conversion has been performed, an Acquirer must register its intent to do so with the Corporation.

POI currency conversion is also referred to as dynamic currency conversion, or DCC. For more information on POI currency conversion, including registration requirements, refer to Chapter 3 of the *Transaction Processing Rules* manual.

5.10 Use of the Marks

A Merchant is only permitted to use a Mark in accordance with a Merchant Agreement with its Acquirer.

The Merchant Agreement must provide that:

1. Any use of a Mark by a Merchant in advertising, acceptance decals, or signs, must be in accordance with the Standards, including the Corporation's reproduction, usage, and artwork Standards, as may be in effect from time to time; and
2. The Merchant's use or display of any Mark will terminate effective with the termination of the Merchant Agreement, or upon notification by the Corporation to discontinue such use or display.

The Acquirer must ensure that its Merchants and ATM owners:

1. Use or display the Marks in accordance with the Standards, and
2. Ceases all use of the Marks immediately upon termination of the Merchant Agreement or ATM Owner Agreement, or upon notification by the Corporation to discontinue such use.

The use or display of any Mark does not give a Merchant or ATM owner any ownership or interest in the Mark.

5.10.1 Display of the Acceptance Marks

An Acquirer must ensure that all of its Merchants and Terminals prominently display the appropriate Acceptance Marks at the Point-of-Interaction (POI), wherever payment options and/or Access Marks are presented.

An Acceptance Mark may also be displayed in advertising or other materials or images at the physical or electronic POI to indicate brand acceptance. No other Marks or marks may be used at the POI to indicate Mastercard, Maestro or Cirrus brand acceptance. An Acquirer must provide its Merchants and ATM Terminal operators with the appropriate artwork in a format authorized by the Corporation. A Merchant may be required to supply its Acquirer with samples of any materials or images bearing the Acceptance Marks.

Refer to the *Mastercard Branding Requirements* at brand.mastercard.com for requirements on displaying the Acceptance Marks at parity with the marks, symbols, and logos of other payment options.

NOTE: Refer to Rule 5.12.1 in the "Additional U.S. Region and U.S. Territory Rules" chapter for a variation to the requirements for display of Acceptance Marks.

5.10.1.1 Location of Display

The Acceptance Marks must be clearly visible to the public at the POI displayed at parity (in terms of size, frequency, color treatment and location) with all other acceptance marks displayed, and, except for e-commerce Transactions as set forth at brand.mastercard.com, afforded similar prominence to any Access Mark displayed (characteristics to consider for similar prominence include size, frequency, color treatment, and co-location within the same field of vision).

The following Standards apply to the acceptance environments specified in the table below:

Acceptance Environment	Acceptance Mark Display Requirements
Face-to-face Transactions	At physical Merchant locations, the preferred way to communicate acceptance is to display the Acceptance Marks on a main entry door or on a nearby window. If these locations are not available, the Acceptance Marks must be displayed so they are seen easily from the outside. When a Cardholder-facing POS Terminal is present at a Merchant location that accepts Mastercard or Maestro or both, the appropriate Acceptance Marks must be displayed on the POS Terminal at parity (in terms of size, frequency, color treatment and location) with all other acceptance marks and afforded similar prominence to any Access Mark displayed (characteristics to consider for similar prominence include size, frequency, color treatment, and co-location within the same field of vision).
Unattended POS Terminals	The Acceptance Marks must be displayed either on the POS Terminal or on its screen, or in both locations.
ATM Terminals	Refer to Rule 4.4.2 for ATM Terminal requirements.
Contactless-enabled POS Terminals	The Acceptance Marks must be displayed in accordance with the "Contactless POS Terminal Branding" section of the *Mastercard Contactless Branding Standards*, which may be found at brand.mastercard.com.
E-Commerce Transactions	The Acceptance Marks must be displayed in accordance with the requirements for digital Merchant locations and digital applications set forth in the *Mastercard Branding Requirements* at brand.mastercard.com.
Submerchant locations	The same requirements apply as for Merchant locations.
Mail order, telephone order, or recurring payment Transactions	For mail order, phone order, and recurring payment Transactions, the Acceptance Marks must be displayed where payment options are presented.
Mastercard Consumer-Presented QR-enabled POS Terminals	The Acceptance Mark must be displayed in accordance with the Mastercard Consumer-Presented QR Branding Standards, which may be found at brand.mastercard.com.

NOTE: Refer to Rule 5.12.1 in the "Additional U.S. Region and U.S. Territory Rules" chapter for a variation to the requirement.

5.10.1.2 Display with Other Marks

Other acceptance marks, symbols, logos, or combinations thereof may appear in the same material or image with the Acceptance Marks, provided visual parity is maintained and no other acceptance mark, symbol, or logo displayed is more prominent or likely to cause confusion concerning the acceptance of Cards.

Each Acceptance Mark must be displayed as a free-standing mark, meaning that an Acceptance Mark must not be displayed so as to suggest that it is either a secondary means of payment or exclusively linked to another acceptance brand.

NOTE: Refer to Rule 4.6 for more information about the Corporation's signage system and the proper display of Acceptance Marks. Refer to Rule 5.12.1 in "Additional U.S. Region and U.S. Territory Rules" for modifications on the use of the Mastercard Brand Mark.

5.11 Merchant Obligations for Acceptance

An Acquirer must ensure that each of its Merchants complies with the Card acceptance requirements set forth in this Rule with respect to the Acceptance Marks specified in the Merchant Agreement.

5.11.1 Honor All Cards

A Merchant must honor all valid Cards without discrimination when properly presented for payment.

A Merchant must maintain a policy that does not discriminate among customers seeking to make purchases with a Card.

A Merchant that does not deal with the public at large (for example, a private club) is considered to comply with this Rule if it honors all valid and properly presented Cards of Cardholders that have purchasing privileges with the Merchant.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "Middle East/Africa Region," and "United States Region" chapters.

5.11.2 Merchant Acceptance of Mastercard Cards

NOTE: Rules on this subject appear in the "Asia/Pacific Region," "Europe Region," "Middle East/Africa Region," and "United States Region" chapters.

5.11.3 Obtain an Authorization

When required by the Standards or by the Acquirer, the Merchant must obtain an authorization before completing a Transaction.

Refer to the *Transaction Processing Rules* manual for authorization requirements.

5.11.4 Additional Cardholder Identification

A Merchant may request but must not require a Cardholder to provide additional identification information as a condition of Card acceptance, unless such information is required to complete the Transaction, such as for shipping purposes, or the Standards specifically permit or require such information to be collected.

A Merchant in a country or region that supports use of the Mastercard Address Verification Service (AVS) for Mastercard POS Transactions may require the Cardholder's ZIP or postal code to complete a Cardholder-Activated Terminal (CAT) Transaction, or the Cardholder's address and ZIP or postal code to complete a mail order, phone order, or e-commerce Transaction.

NOTE: A modification to this Rule appears in the "United States Region" chapter.

5.11.5 Discounts or Other Benefits at the Point of Interaction

NOTE: Rules on this subject appear in the "Asia/Pacific Region," "Canada Region," "Europe Region," "Latin America and the Caribbean Region," and "Middle East/Africa Region" chapters.

5.11.6 Merchant Business Logos

The Corporation may from time to time make additional data available to the Issuer in order to enrich the posting of Transaction data with publicly available business information pertaining to a Merchant or Submerchant.

For purposes of example and not limitation, such information may include geographic mappings of physical business addresses, publicly disclosed contact information, sales policies, and other such publicly available business information.

To enable greater transparency and reduce fraud for the benefit of all participants in the Interchange System, the Acquirer must refer all of its Merchants and Submerchants to the Mastercard Logo Microsite (https://logo.ethoca.com) for purposes of providing the Corporation with business logos for use by the Corporation in accordance with the agreed terms and conditions from the Mastercard Logo Microsite.

5.12 Prohibited Practices

An Acquirer must ensure that none of its Merchants engage in any of the prohibited practices set forth in this Rule.

5.12.1 Discrimination

A Merchant must not engage in any acceptance practice that discriminates against or discourages the use of a Card in favor of any other acceptance brand.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "United States Region," and "Additional U.S. Region and U.S. Territory Rules" chapters.

5.12.2 Charges to Cardholders

A Merchant must not directly or indirectly require any Cardholder to pay a surcharge or any part of any Merchant discount or any contemporaneous finance charge in connection with a Transaction.

A Merchant may provide a discount to its customers for cash payments. A Merchant is permitted to charge a fee (such as a bona fide commission, postage, expedited service or convenience fees, and the like) if the fee is imposed on all like transactions regardless of the form of payment used, or as the Corporation has expressly permitted in writing.

For purposes of this Rule:

1. A surcharge is any fee charged in connection with a Transaction that is not charged if another payment method is used.
2. The Merchant discount fee is any fee a Merchant pays to an Acquirer so that the Acquirer will acquire the Transactions of the Merchant.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Canada Region" and "Additional U.S. Region and U.S. Territory Rules" chapters.

5.12.3 Minimum/Maximum Transaction Amount Prohibited

A Merchant must not require, or indicate that it requires, a minimum or maximum Transaction amount to accept a valid and properly presented Mastercard or Maestro Card.

NOTE: A modification to this Rule appears in the "Additional U.S. Region and U.S. Territory Rules" chapter.

5.12.4 Scrip-dispensing Terminals

The Acceptance Marks must not be displayed at any POS Terminal, ATM Terminal, or Bank Branch Terminal that dispenses scrip.

A Merchant must not submit to its Acquirer, and an Acquirer must not submit to the Interchange System, any Transaction that arises from the acceptance of a Card at a scrip-dispensing Terminal.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

5.12.5 Existing Mastercard Cardholder Obligations

A Merchant must not submit to its Acquirer, and a Customer must not submit to the Interchange System, any Transaction that:

1. Represents the refinancing or transfer to a credit Card of an existing Mastercard Cardholder obligation that is deemed to be uncollectible; or
2. Arises from the dishonor of a Mastercard Cardholder's personal check.

The Acquirer may use MCC 6051 (Quasi-Cash: Merchant) to identify a Transaction for the payment of an existing Cardholder obligation owed to the Merchant.

A Transaction that represents the refinancing or transfer of an existing Cardholder obligation that has been deemed uncollectible may be effected with a Debit Mastercard or Maestro Card, including any prepaid Card.

For purposes of this Rule, an obligation is deemed uncollectible when it has been charged off or sold to another institution for the purpose of full or partial debt recovery and does not represent a payment for goods or services provided by the Merchant. The Acquirer may use MCC 7322 (Debt Collection Agencies) to identify Transactions for the payment of such Cardholder obligations.

NOTE: Modifications to this Rule appear in the "Europe Region" chapter.

5.12.6 Cardholder Right of Dispute

A Merchant must not impose, as a condition of Mastercard or Maestro Card acceptance, a requirement that the Cardholder waive a right to dispute a Transaction.

5.12.7 Illegal or Brand-damaging Transactions

A Merchant must not submit to its Acquirer, and a Customer must not submit to the Interchange System, any Transaction that is illegal, or in the sole discretion of the Corporation, may damage the goodwill of the Corporation or reflect negatively on the Marks.

The Corporation considers any of the following activities to be in violation of this Rule:

1. The sale or offer of sale of a product or service other than in full compliance with law then applicable to the Acquirer, Issuer, Merchant, Cardholder, Cards, or the Corporation.
2. The sale of a product or service, including an image, which is patently offensive and lacks serious artistic value (such as, by way of example and not limitation, images of nonconsensual sexual behavior, sexual exploitation of a minor, nonconsensual mutilation of a person or body part, and bestiality), or any other material that the Corporation deems unacceptable to sell in connection with a Mark.

An Acquirer that has been notified of a Merchant's noncompliance with this Rule and that fails promptly to cause the noncompliant practice to cease, or that has been notified multiple times regarding violations of this Rule, is subject, at the Acquirer's expense, and in addition to any

other noncompliance assessment or other discipline, or both, to any one or more of the following:

1. Customer Risk Review under the Global Risk Management Program as described in the *Security Rules and Procedures* manual.
2. An audit at the sole expense of the Acquirer by a third party selected by the Corporation, of the Acquirer's acquiring practices. The Corporation may list a Mastercard Merchant which the Corporation determines is noncompliant with this Rule on the MATCH system. (See Chapter 11 of the *Security Rules and Procedures* manual.)

In addition to or in lieu of any other disciplinary action by the Corporation, an Acquirer deemed to be in violation of this Rule may be assessed, with respect to each Merchant, entity, affiliate, agent, or person on whose behalf the Acquirer submits illegal or brand-damaging Transactions into interchange:

- USD 200,000 or
- USD 2,500 per day, retroactive to the first day of the noncompliant practice, provided the Acquirer can show clear and convincing evidence that such noncompliant practice began less than 80 days prior to the date of the Corporation's notification to the Acquirer.

5.12.8 Disparagement

NOTE: A Rule on this subject appears in the "Additional U.S. Region and U.S. Territory Rules" chapter.

5.12.9 Mastercard Tokens

Neither an Acquirer nor any of the Acquirer's Merchants or Service Providers, including but not limited to any such entity that the Corporation has registered as a Token Requestor, may use Account or Transaction data to create or maintain a repository of Mastercard Token primary account numbers (PANs) and corresponding Account PANs or perform mapping of Mastercard Token PANs to Account PANs for any purpose.

The PAN of a Mastercard Card or Access Device or any Maestro Card or Access Device for which Maestro is the primary Payment Application must not be replaced by, mapped to, or Tokenized with any PAN issued from an Issuer Identification Number (IIN) reserved by the ISO Registration Authority for a competing payment network. Refer to the current *ISO Register Of Issuer Identification Numbers* for more information.

5.13 Valid Transactions

A Merchant must submit to its Acquirer records of valid Transactions only between the Merchant and a bona fide Cardholder.

A Merchant must not submit to its Acquirer a Transaction that the Merchant knows or should have known to be fraudulent or not authorized by the Cardholder, or that it knows or should have known to be authorized by a Cardholder colluding with the Merchant for a fraudulent purpose. For purposes of this Rule, the Merchant is deemed to be responsible for the conduct of its employees, agents, and representatives.

5.14 Sale or Exchange of Information

A Merchant must not sell, purchase, provide, exchange or in any manner disclose Account or Transaction data, including but not limited to the Account PAN, PAR, or Token, or personal information of or about a Cardholder to anyone other than its Acquirer, to the Corporation, or in response to a valid government demand.

This prohibition applies to Card imprints, TIDs, carbon copies, mailing lists, tapes, database files, and all other media created or obtained as a result of a Transaction.

5.15 Payment Account Reference (PAR) Data

This Rule 5.15 applies whether the Corporation or another entity as BIN Controller (as such term is defined in the EMV Payment Tokenization Specification Technical Framework) allocates a Payment Account Reference (PAR) value to an Account PAN.

An Acquirer, and any of the Acquirer's Service Providers or Merchants, must only use PAR data for one or more of the following purposes:

- To complete a refund, respond to a chargeback, or perform some other reversal of payment in connection with a purchase Transaction containing a PAR, in addition to an Account PAN or Token;
- To comply with applicable law or regulation or the Mastercard Anti-Money Laundering Program;
- To conduct fraud detection, control, or mitigation activities;
- To provide services to a Cardholder at the direction of and with the explicit consent of such Cardholder.

No other use of PAR data is permitted without the express prior written consent of the Corporation.

Chapter 6 Issuing Activity

This chapter contains Rules relating to the issuance of Cards, Issuer obligations, and Special Issuer Programs.

6.1 Card Issuance—General Requirements

An Issuer must operate each of its Programs in accordance with the Standards as may be in effect from time to time.

Each Program must be:

- Structured so as to avoid undue risk to the Corporation and its Customers; and
- Operated in a manner that does not reflect poorly on the Corporation or any Mark.

An Issuer must ensure that a Card or Access Device:

1. Only provides access to an eligible account type;
2. Displays the appropriate Brand Marks pursuant to the applicable License and the Standards, including the *Card Design Standards* manual and all other reproduction, usage and artwork Standards;
3. Complies with the Standards set forth in Chapter 3 of the *Security Rules and Procedures* manual;
4. If it contains a chip or has contactless payment functionality, complies with the Standards set forth in the *M/Chip Requirements for Contact and Contactless* manual; and
5. If it supports Mastercard Consumer-Presented QR payment functionality, complies with the Standards set forth in the *M/Chip Requirements for Contact and Contactless* manual and the Mastercard Cloud-Based Payments (MCBP) documentation.

There is no limitation on the types of Accounts that may co-reside on the same Mobile Payment Device, provided that such Accounts are not linked, but rather exist independently and are each accessed by a separate and distinct Payment Application hosted on the same user interface.

Mastercard Crypto Secure

All Issuers must monitor, assess, and mitigate the risk in their Mastercard Card Portfolios that is associated with Processed Transactions for the purchase of crypto assets.

Issuers are required to participate in Mastercard Crypto Secure to comply with this Standard.

Participation in Mastercard Crypto Secure is an Activity, and as such, is subject to Standards applicable to Activity, including Rule 2.3. The Corporation is not liable for any Issuer's losses arising from the use of or failure to use Mastercard Crypto Secure.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," "Latin America and the Caribbean Region," and "Middle East/Africa Region" chapters.

Mastercard Safety Net

All Issuers must participate in Mastercard Safety Net, or Mastercard Safety Net alerts, for both Processed Transactions and Transactions not authorized, cleared, and settled via the Interchange System. For the avoidance of doubt, this (i) includes any Transaction effected through the utility of a Mark or Mastercard-branded Application Identifier (AID) with a Card issued under a Corporation-assigned BIN (refer to Rule 3.17), and (ii) excludes any transaction

effected through the utility of the brand or Application Identifier (AID) of a co-badged payment scheme (i.e., a scheme whose mark appears together with a Mark on the applicable Card).

Participation in Mastercard Safety Net and Mastercard Safety Net alerts is Activity, and as such, is subject to Standards applicable to Activity, including Rule 2.3. The Corporation is not liable for any Issuer's fraud losses arising from the use of Mastercard Safety Net or Mastercard Safety Net alerts.

NOTE: For the applicability of these Mastercard Safety Net requirements for non-Processed Transactions in a Region, refer to the Region chapter.

Transaction Alerts Service

An Issuer must offer a Transaction alerts service to its Cardholders as set forth in this Rule, when applicable.

NOTE: For modifications to these Transaction alert service requirements in a Region, refer to the Region chapter.

A Transaction alerts service is a service that alerts the Cardholder to the use of a Card for which he or she is the authorized user. A Transaction alerts service must:

- Provide the Cardholder with the option to activate the Transaction alerts service;
- Allow the activation of Transaction alerts by individual Account PAN; and
- Allow the Cardholder to set parameters for Transaction alerts based on authorization activity which, at a minimum, must include the Transaction amount.

It is strongly recommended that an Issuer support Transaction alerts:

- For Cross-border Transactions; and
- By Transaction type (for example, e-commerce Transactions, mail order/telephone order Transactions) or channel (for example, Card-not-present Transactions) or both.

The Issuer's offering of a Transaction alerts service is:

- Required for all consumer Cards except prepaid Cards for which the Issuer does not collect, store, or otherwise validate the consumer's identity pursuant to the *Guidelines for Anonymous Prepaid Card Programs* available on Mastercard Connect;
- Required for commercial Cards issued for use by a small or mid-sized business (as defined by the Corporation) in certain Regions; and
- Optional for commercial Cards issued for use by a large business (as defined by the Corporation).

NOTE: For more information about commercial Cards for small, mid-sized, and large businesses, refer to www.mastercard.com.

Mastercard Decision Intelligence

NOTE: A Rule on this subject appears in the "Asia/Pacific Region" chapter.

Mastercard Acquirer Fraud Dashboard

NOTE: A Rule on this subject appears in the "Asia/Pacific Region" chapter.

6.1.1 Mastercard Card Issuance

The following requirements apply to the issuance of Mastercard Cards:

1. If an approved Cardholder application for issuance of a payment card or access device indicates the applicant's preference, by way of a checkmark or otherwise, to be issued a Mastercard Card, then the Issuer must issue a Mastercard Card.
2. In conjunction with Mastercard Card issuance, the Issuer must provide a personal identification number (PIN) or offer the Cardholder the option to receive or select a PIN for purposes of Account access at ATM Terminals. PIN verification may also be supported for Chip Transactions. Refer to section 3.4, "Mastercard Cardholder Verification Requirements" in the *Transaction Processing Rules* manual regarding the use of PIN for magnetic stripe POS Transactions.
3. An Issuer must ensure that each newly issued or re-issued contactless-enabled Mastercard Card and Access Device is personalized with the appropriate device type value.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Canada Region," "Middle East/Africa Region," and "United States Region" chapters.

6.1.1.1 Linked Mastercard Card Program Solicitations

Without the express prior written consent of the Corporation, an Issuer must not use a Solicitation or conduct any advertising, promotion, marketing, or the like in connection with a Mastercard Card Program that is in any way linked to a different payment card.

6.1.2 Maestro Card Issuance

The following requirements apply to the issuance of Maestro Cards:

1. The Issuer must maintain the funds in the Maestro Account.
2. The Issuer must not place the Maestro Brand Mark on any card that has access to any of the following types of accounts:
   a. A charge card or credit card account as the primary account; or
   b. Accounts that "pass-through" to an account at an institution not eligible to be a Customer.
3. In conjunction with Maestro Card issuance, the Issuer must provide a PIN or allow the Cardholder to select a PIN.
4. An Issuer must verify its Cardholders by means of online PIN verification as the CVM if a magnetic stripe is used to initiate the Transaction, except under the circumstances outlined in section 3.5, "Maestro Cardholder Verification Requirements" of the *Transaction Processing Rules* manual.
5. Chip Cards must support both online PIN verification and offline PIN verification for POS Transactions.

6. An Issuer must ensure that each newly issued or re-issued contactless-enabled Maestro Card and Access Device is personalized with the appropriate device type value.

NOTE: Modifications to this Rule appear in the "Canada Region," "Europe Region," "Latin America and the Caribbean Region," and "United States Region" chapters.

6.1.2.1 Eligible Accounts—Maestro

The Issuer must ensure that the account to which a Maestro Card provides access, directly or indirectly, through the Mastercard® ATM Network is one of the following:

Any checking, savings, NOW, current, sight deposit, share draft accounts (and overdraft lines of credit linked to such accounts), or pooled accounts (linked to a Corporation-approved prepaid Card Program) maintained by or on behalf of a Cardholder with an Issuer.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

6.1.2.2 Ineligible Accounts—Maestro

Any account held or serviced by a Maestro Customer Licensed to conduct only acquiring Activity is not eligible to be a Maestro Account.

This provision does not prevent a Customer from using the Mastercard® ATM Network for Gateway Processing, if such use has been authorized by the Corporation and is expressly permitted in the Standards.

6.1.3 Cirrus Card Issuance

Any card that permits its holder to obtain access to one or more eligible Accounts, as described in Rule 6.1.3.2, through the Mastercard® ATM Network is a Cirrus Card and must display the appropriate Brand Marks in accordance with the Standards.

The following requirements apply to the issuance of Cirrus Cards:

1. In conjunction with Cirrus Card issuance, the Issuer must provide a PIN or allow the Cardholder to select a PIN.
2. The Issuer determines the maximum cash withdrawal limits applicable to its Cardholders; however, with respect to a Mastercard credit Card bearing the Cirrus Brand Mark, the Issuer must permit the Cardholder to withdraw at least the equivalent of USD 200 daily if the available credit exists, and there is no other reason to deny the Transactions.

A Program offering Cirrus Cards must satisfy the following additional criteria:

1. The Customer issuing the Card must hold the Account accessed by the Card.
2. The Issuer must fund all of the credit card loans and own the accounts receivable for the Program, provided, however, that "securitization" of credit card receivables does not disqualify a Program.
3. The Issuer must have an unconditional right to demand the surrender of its Cards.

6.1.3.1 Eligible Cards—Cirrus

A Customer must obtain the express prior written consent of the Corporation before any card not described in the following list may be issued or otherwise participate in the Mastercard® ATM Network as a Cirrus Card:

1. A card issued in the name or trade name of a Customer to its depositors or electronic benefits transfer ("EBT") recipients in Corporation-approved programs, provided that such cards access only:
   a. A deposit account held by such Customer;
   b. An overdraft credit line extended to such Customer; or
   c. A brokerage or money market mutual fund account that is authorized by this Rule 6.1.3.1.
2. A card issued in the name or trade name of a Customer to employees of any of its corporate depositors to provide access to such corporate depositors' accounts as authorized by such corporate depositor.
3. A Mastercard credit Card or Visa credit card bearing the name or trade name of a Customer and which provides access to credit accounts held or serviced by such Customer, including those bearing the name of a non-Customer Partner as set forth in Rule 6.6.
4. A private label credit card that complies with all Cirrus Card design Standards and clearly discloses the identity of the Issuer.
5. A Diners Club card issued by participating franchises.
6. A card issued in the name or trade name of a Customer, to the Customer's customers, provided that such card affords access only to loan accounts held by such Customer. Such cards must not be used for credit purchases or to provide access to so-called "pass-through," "sweep," or "zero-balance" accounts for which the funds or credit ultimately come from entities not eligible for participation in the Corporation.

The limitations contained in this Rule do not apply to a loan account or deposit account linked to a mutual fund investment, provided there is a meaningful relationship between the Customer and the Cardholder, and the Card does not bear any name, trade name or trademark of an entity that is ineligible for participation in the Corporation. For purposes of this Rule, indicators of a meaningful relationship between the Customer and the Cardholder include, without limitation, the following:

1. A written agreement regarding the account between the Customer and the Cardholder;
2. The right of the Customer unilaterally to discontinue the account relationship with the Cardholder;
3. Periodic statements for the account issued by the Customer directly to the Cardholder in the Customer's name;
4. Management of the account and Cardholder relationship by employees of the Customer; and
5. An active, Customer-driven program to market the product (for example, an investment vehicle with account access).

6.1.3.2 Eligible Accounts—Cirrus

The Issuer must ensure that the account to which a Card provides access through the Mastercard® ATM Network is one of the following:

1. Any checking, savings, NOW, current, sight deposit, share draft accounts (and overdraft credit lines linked to such accounts), credit accounts, or pooled accounts (linked to an Corporation-approved prepaid Card Program) maintained by or on behalf of a Cardholder with an Issuer;
2. An account of a securities brokerage firm that is a member of the National Association of Securities Dealers, if such firm is also a subsidiary of a bank holding company, a multiple savings and loan holding company whose activities are restricted in accordance with 12 U.S.C. § 1467a(c)(1), as amended, or a unitary savings and loan holding company operating pursuant to 12 U.S.C. § 1467a(c)(3), as amended;
3. An account of a money market mutual fund registered in the United States with the Securities and Exchange Commission as an open-ended investment company under the Investment Company Act of 1940, as amended, if the investment adviser or administrator of such fund is a subsidiary of a bank holding company, a multiple savings and loan holding company whose activities are restricted in accordance with 12 U.S.C. § 1467a(c)(1), as amended, or a unitary savings and loan holding company operating pursuant to 12 U.S.C. § 1467a(c)(3), as amended; or
4. A credit account held or serviced by a Customer.

The Corporation may require guarantees and other assurances that brokerage firms and mutual funds described in parts 2 and 3 of this Rule will meet their settlement and other obligations to the Corporation and its Customers. Programs that involve the issuance of Cards that access accounts of a securities brokerage firm or a money market mutual fund must be approved by the Corporation in writing prior to their inauguration, if such brokerage firm is owned or such mutual fund is advised by a subsidiary of a unitary savings and loan holding company. At a minimum, an Issuer must provide each Cardholder, wherever domiciled, with Account access in the country where such Issuer is Licensed.

6.1.3.3 Ineligible Cards—Cirrus

A card is ineligible to be a Cirrus Card if:

1. The card bears the name, trade name, trade mark or other service mark of a Competing ATM Network and is used to initiate Gateway Processing, or if such card, without such identification of a Competing ATM Network, is an access device for such a Competing ATM Network.
2. In the opinion of the Corporation, and notwithstanding items 1 through 6 in the first paragraph of Rule 6.1.3.1, the card provides its holder with access to products or services that a commercial bank could not make available to the holders of its cards on an identical and competitive basis, or if the appearance of such card is likely to cause confusion regarding participation in the Corporation.
3. Except as provided in item 6 in the first paragraph of Rule 6.1.3.1, the card provides access to or the account is a so-called "pass-through," "sweep," or "zero-balance" account, for which the funds or credit ultimately come from an entity ineligible to be a Customer of the

Corporation. The limitation set forth in the preceding sentence does not apply to a deposit account linked to a mutual fund investment if:

a. There is a meaningful relationship between the Customer and the Cardholder, as described in Rule 6.1.3.1; and
b. The Card that accesses such account does not bear any name, trade name or trademark of an entity that is ineligible for participation in the Corporation.

6.1.3.4 Ineligible Accounts—Cirrus

Any account held or serviced by a Cirrus Customer Licensed to conduct only acquiring Activity is not eligible to be a Cirrus Account.

This provision does not prevent a Customer from using the Mastercard® ATM Network for Gateway Processing, if such use has been authorized by the Corporation and is expressly permitted in the Standards.

6.1.3.5 Transferred Cirrus Portfolios

A Cirrus Card that is part of a Portfolio that has been transferred by a Customer to an entity that is ineligible to be a Customer of the Corporation may continue to be a Cirrus Card during its withdrawal period subject to compliance with the Standards, including but not limited to Rule 1.10.

6.1.4 Tokenization of Accounts

With respect to the Tokenization of Accounts, all of the following applies:

1. The Corporation has the sole right to designate a Mastercard Token Account Range to an Issuer.
2. Each Mastercard Token must be allocated by the Corporation, unless the Corporation has expressly approved otherwise.
3. The Tokenization of an Account primary account number (PAN) must be performed in compliance with all applicable Standards, including but not limited to the Mastercard Token Service Provider Standards.
4. Mastercard must be provided the mapping between the PAN assigned to a Card, and each Mastercard Token associated with the Account for use by the authorized user of the Card.
5. An Account PAN must be Tokenized whenever a Mobile Payment Device, Access Device, or other non-Card method is used, in addition to a Card, to provide access to an Account.
6. The PAN of a Mastercard Card or Access Device or any Maestro Card or Access Device for which Maestro is the primary Payment Application must not be replaced by, mapped to, or Tokenized with any PAN issued from an Issuer Identification Number (IIN) reserved by the ISO Registration Authority for a competing payment network. Refer to the current *ISO Register Of Issuer Identification Numbers* for more information.
7. The Mastercard Token cryptogram, when present, must be validated during the authorization of all Transactions involving Tokenized Accounts.

An Issuer wishing to support the Tokenization of its Accounts for use on a Mobile Payment Device must:

1. Comply with all technical specifications and other Standards applicable to Tokenization and Digitization;
2. Complete all testing and certifications as may be required by the Corporation from time to time in connection with Tokenization and Digitization;
3. Decline any request to Tokenize an Account if:
   a. The identity of the Cardholder is unknown to the Issuer;
   b. The Token Requestor is not a Digital Activity Customer or other Customer approved by the Corporation to conduct Digital Activity; or
   c. The geographic location of the Cardholder if and as provided by the Token Requestor is an OFAC-sanctioned location; and
4. Establish Cardholder support policies and procedures.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region," "Europe Region," and "United States Region" chapters.

6.1.4.1 Maestro Accounts

NOTE: A Rule on this subject appears in the "United States Region" chapter.

6.1.5 Cardholder Communications

A Customer must comply with the Corporation's Cardholder Communication requirements, including but not limited to those set forth in Rule 6.2.1.

Each Program Solicitation must:

1. Refer prominently to the offering exclusively as a Card and not position the offering as anything other than a Card;
2. Prominently feature the Word Marks and Brand Marks of the Card Program;
3. Clearly disclose the identity of the Card Issuer; and
4. Not position the Program name or logo as adding superior utility to the Card.

6.1.6 Enablement of QR-based Payments

NOTE: A Rule on this subject appears in the "Asia/Pacific Region" chapter.

6.2 Issuer Responsibilities to Cardholders

An Issuer must provide information to its Cardholders as set forth below.

1. **Card Solicitations.**
   Each Issuer of Cards must disclose, clearly and conspicuously, in all Solicitations any amounts relating to the Issuer Cross-border Assessment and/or the Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
2. **Cardholder Communications.**

Each Issuer of Cards must disclose, clearly and conspicuously, in all new and existing Cardholder Communications, including Cardholder agreements and Account agreements, any amounts relating to the Issuer Cross-border Assessment and/or the Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.

3. **Periodic Billing Statement.**
   Each Issuer of Cards must provide adequate disclosure on each applicable periodic billing statement, such that the Cardholder can readily determine from the billing statement any amounts that the Issuer charges to the Cardholder relating to the Issuer Cross-border Assessment and/or the Currency Conversion Assessment during that billing cycle, either in gross or on a per Transaction basis.
4. **Currency Conversion Procedure.**
   The Corporation further recommends and encourages Issuers to inform their Cardholders that the Corporation's currency conversion procedure is based on rates observed in the wholesale market or government-mandated rates, where applicable. The currency conversion rate that the Corporation uses for a particular Transaction is the rate for the applicable currency on the date that the Transaction occurred. However, in limited situations, particularly where Transaction submissions to the Corporation for processing are delayed, the currency conversion rate that the Corporation uses may be the rate for the applicable currency on the date that the Transaction is processed (the Central Site Business Date).

For information about the Currency Conversion Assessment, refer to the *GCMS Reference Manual* or *Single Message System Specifications*. For information about the Cross-border Assessment, refer to the Pricing and Billing Center on Mastercard Connect™.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

6.2.1 Cardholder Communications

Each Cardholder Communication provided to a prospective Cardholder must:

- Clearly disclose the terms and conditions of the Card Program and the identity of the Customer as the Card Issuer; and
- Otherwise be clear and truthful and not reflect poorly on the Corporation or any Mark.

6.3 Limitation of Liability of Cardholders for Unauthorized Use

An Issuer must not hold a Cardholder liable for a Transaction that was not authorized by the Cardholder if the Cardholder exercised reasonable care in safeguarding the Card from risk of loss or theft and, upon becoming aware of such loss or theft, promptly reported the loss or theft to the Issuer.

This Rule shall not apply to a Transaction conducted with a Card that is:

1. Issued to an entity other than a natural person or for a commercial purpose, except that the Rule shall apply to Cards issued for use by a small business (including, for purposes of example and not limitation, the following: Debit Mastercard Business Card®, Mastercard

Business Card®, Mastercard Business Prepaid Card, and World Elite Mastercard® for Business); or

2. Issued and/or sold to a person until such time as that person's identity is registered by or on behalf of the Issuer in connection with such issuance and/or sale, which registration may include Customer identification program requirements.

If applicable law imposes a greater liability or a conflicting obligation, such applicable law shall govern.

6.4 Selective Authorization

Without the express prior written approval of the Corporation, a Customer must not launch or maintain a Card Program that has the effect of selectively authorizing Transactions arising from use of the Cards and Accounts at only a subset of Mastercard or Maestro acceptance locations.

A Customer may authorize or decline individual Transactions based on:

1. The amount of funds or credit available;
2. Fraud or credit risks presented by individual Cardholder usage patterns;
3. Cash access restrictions to manage a secured or high risk account;
4. Cardholder-designated restrictions on use; or
5. Any other restriction on use the Corporation may permit.

An Issuer's authorization decision must be made on an individual Transaction basis and not on the basis of Merchant or Terminal country location, Acquirer country location, Transaction type, acceptance environment, or other similar factors except as permitted by the Standards (although any such factors or combination thereof may contribute to the decision).

Notwithstanding the foregoing, a Customer is permitted to issue a Contactless Payment Device that provides access to a Mastercard or Maestro Account without also issuing an accompanying Card in connection with or which links to the same Account. Any Contactless Payment Device issued without an accompanying Card must support Transactions of any amount, and the Issuer must provide clear instructions to the Cardholder as to the limitations of its use.

NOTE: Modifications to this Rule appear in the "Europe Region" chapter.

6.5 Affinity and Co-Brand Card Programs

A Mastercard, Maestro, or Cirrus Card Program may be issued as an Affinity Card Program or Co-Brand Card Program.

As set forth in the *Card Design Standards*, an Issuer may use the area on a Card front reserved for the identification of the Issuer to instead or additionally identify a person or entity other than the Issuer. Such person or entity is referred to herein as a "Partner." There are two types of Partners: an "Affinity Group," which is an educational or other not-for-profit entity that

promotes an institution or activities, and a "Co-brand Partner," which is a for-profit company organized to engage in commercial activity.

NOTE: Modifications to this Rule appear in the "Europe Region" chapter.

6.5.1 Ownership and Control of the Program

An Affinity Card Program or Co-brand Card Program must be entirely owned and Controlled by the Issuer at all times, and a Partner must not own or Control any part of the Program or the Program receivables. However, the assignment of receivables or sale of a participation in receivables to the Partner, or some other financing vehicle involving the Partner, is permitted provided the Program is owned and Controlled by the Customer.

The Corporation exclusively determines if an Issuer is in compliance with the foregoing requirements. In making such a determination, the Corporation may consider such factors as:

1. Whether the Customer establishes the Program policies and guidelines, such as Cardholder credit and eligibility decisions;
2. The Customer's role in setting fees and rates;
3. What the Customer has at risk;
4. Whether the Customer actively ensures that the Program policies and guidelines are implemented;
5. The ownership and Control of the Program receivables;
6. Whether all or a substantial portion of the receivables are financed with the Partner; and
7. The extent to which the Customer, and not the Partner, is portrayed as the owner of the Program.

6.5.2 Use of the Acceptance Marks

An Acceptance Mark displayed at the POI must appear apart from any Partner identification and must at least have parity in size and prominence with any Program logo, Program name, or the like, and with any competing mark also displayed.

The Corporation has the right to require the modification or removal of any POI display of a Program name or logo that the Corporation determines does not comply with this Rule or reflects negatively on any Mark.

6.6 Brand Value Transactions and Proprietary Accounts

A Brand Value Transaction ("BVT") means a Customer or third party transaction that originates by the use of a Mastercard Card to access a proprietary account, proprietary application, or both.

A BVT is a transaction that may:

1. Access a proprietary account through use of an Affinity Card Program or Co-brand Card Program Mastercard Card at the Partner's own Merchant locations or at other Merchants that participate in the Partner's services;

2. Access proprietary stored value residing on a Mastercard Card's magnetic stripe or chip; or
3. Use a non-payment application residing on a Mastercard Card, such as a loyalty application, an electronic coupon, medical information, or paperless ticketing. The technology employed by the non-payment application must not facilitate or otherwise enable the use of a competitive payment product for the non-payment benefit or service.

6.6.1 Proprietary Account Access

A proprietary account number may have one or more of the following characteristics:

1. The proprietary account number is different from the primary account number (PAN) associated with the Mastercard Account. The proprietary account number may appear on the Card face, be encoded on the Card, or be cross-referenced in the Customer or a Partner's system.
2. The proprietary account number is used in a system or network for authorization and settlement that is distinct from the Interchange System and is not used in the Interchange System.
3. Any billing related to use of the proprietary account number is distinct from any billing for the Mastercard Account, whether as part of a common statement or in a separate statement.

A Program Card must provide the Cardholder access to the same proprietary account that the Partner previously established for the Cardholder, for payment of the same particularly defined set of transactions that were previously payable by other means.

6.6.2 Use of BVT and Proprietary Accounts on a Mastercard Card

A BVT, as defined by the Corporation, may be present on a Mastercard Card for the following functionalities:

1. Enable access to a proprietary ATM network
2. Prepaid phone and long distance calling purses
3. Proprietary meal plan purses
4. Proprietary transit system payments
5. Accessing proprietary stored value, in accordance with Standards applicable to permitted forms of Electronic Money
6. Previously approved Programs so long as the properties and purpose of the Program does not change. The Corporation reserves the right to impose changes or revoke these approvals at any time.
7. Any functionality otherwise expressly approved in writing by the Corporation

A proprietary account, as exclusively defined by the Corporation, may be present on a Mastercard Card for the following functionalities:

1. Campus cards
2. Door access devices
3. Loyalty applications
4. Cardholder reference numbers

5. Electronic coupons
6. Medical information
7. Paperless ticketing
8. Previously approved Programs so long as properties and purpose of program does not change. The Corporation reserves the right to impose changes or revoke these approvals at any time.
9. Any functionality otherwise expressly approved in writing by the Corporation.

The Corporation exclusively determines if a BVT or proprietary account number may be used on a Mastercard Card.

6.6.3 Fees and Reporting Requirements

From time to time, the Corporation may establish, implement, and collect fees, assessments, or both arising from or related to BVTs, proprietary accounts, or both.

If a BVT involves an Affinity Card Program or a Co-brand Card Program, the Customer must separately report to the Corporation the number of Cards outstanding, the proprietary account sales volume on such Cards, and any other requested information in the form and at such times as the Corporation requires.

6.7 Virtual Accounts

A Virtual Account is a Mastercard Account issued without a physical Card or Access Device. A Virtual Account cannot be electronically read.

For the avoidance of doubt, an Account PAN Tokenized for use on a Mobile Payment Device is not considered a Virtual Account.

Subject to the requirements set forth below, a Customer is not required to issue a physical Card in connection with or which links to a Virtual Account.

An Issuer of a Virtual Account must comply with all of the following requirements:

1. A Virtual Account must be assigned a 16-digit primary account number (PAN) in conformance with the Standards applicable to Mastercard Cards, and must be assigned a Card Validation Code 2 (CVC 2) value and an expiration date.
2. A reference device may be used to communicate this information, but must not be designed in a manner that may cause consumer or acceptance confusion with a Card (such as the inclusion of artwork that would resemble a magnetic stripe, EMV chip, or Mastercard hologram product). For reference device design Standards, refer to the *Card Design Standards* manual.
3. A Virtual Account must be enhanced with Address Verification Service (AVS) when the Account is issued for use in an area where AVS is available.
4. Partial approval authorization service must be supported for all prepaid and Debit Mastercard (including prepaid) Virtual Account ranges.

5. Before activating a Virtual Account, the Issuer must communicate to the Cardholder the PAN and the expiration date of the Account, the identity of the Issuer, and instructions as to the manner in which the Virtual Account may be used.

The Corporation recommends that the Issuer prominently disclose upon issuance that the Virtual Account should not be used to purchase an item over the Internet that subsequently would require presentment of a physical reference device in order to obtain that item. Examples include certain theater ticket purchases, hotel stays, car rentals, and online purchases picked up in person.

6.8 Secured Card Programs

A secured Mastercard Card means a Mastercard Card for which a line of credit is secured by an amount held on deposit.

6.8.1 Refund of Fees

If a Customer promises, directly or indirectly, to refund any fee paid by an applicant for a secured Mastercard Card if the Card is not so issued, the Customer must ensure that such refund is made promptly and in any event within 30 days following the submission of the application and without any further action by the applicant.

6.8.2 Solicitation and Disclosure Requirements

The following Solicitation and disclosure requirements apply to a secured Mastercard Card Program:

1. A Customer that conducts a secured Mastercard Card Program without the use of a Service Provider may use a Program name to identify such a Program, in addition to or in lieu of the Customer's name, subject to the prior written approval of the Corporation.
2. A Solicitation must not reference consumers who have filed, or are contemplating filing, for bankruptcy relief. Any reference within a Solicitation to a consumer's credit problem may be included only in the general disclosure to the consumer.
3. Each Solicitation for a secured Mastercard Card must clearly and conspicuously disclose that the Card is a secured Mastercard Card and that the consumer must establish a deposit account. The Solicitation also must specify that the credit line will be equal to either the amount of the security deposit, or a specified percentage of the security deposit.
4. No Solicitation may refer to a specific credit line limit unless the Issuer
   a. Regularly issues secured Mastercard Cards with such a credit limit, or
   b. Has in effect a policy that (i) permits the regular issuance of secured Mastercard Cards with such a credit limit, and (ii) is compatible with the Issuer's policy governing its issuance of secured Mastercard Cards with lower credit limits.
5. Each Solicitation for a secured Mastercard Card must clearly and conspicuously disclose what an applicant will receive by responding to the Solicitation. If the applicant is not issued a secured Mastercard Card after responding to a Solicitation, this fact must be clearly and conspicuously disclosed in the Solicitation.

6. Each Solicitation for a secured Mastercard Card must clearly and conspicuously disclose any and all application or other fees the applicant must pay, or could be required to pay, to be issued a secured Mastercard Card. All such fees must be made payable to the Issuer and not to any other person or entity.

6.9 Youth Card Programs

Solely for the purposes of Rule 6.9 and 6.9.1, the following terms have the meanings set forth below:

1. "Minor" or "Youth" means a person under the age of majority as determined in accordance with laws and/or regulations applicable to the place where the Primary Cardholder then resides or any person under the age of fifteen in the place where the Primary Cardholder then resides where age of majority is not expressly defined under local law.
2. "Primary Cardholder" means the Cardholder authorized to use the Card and to be financially responsible for the Card.
3. "Youth Card" means a Card issued to a Minor as a Primary Cardholder. For clarity, a Card issued to a Minor at the request of the Primary Cardholder and bearing the same Primary Account Number as the Card issued to the Primary Cardholder is not a Youth Card if the Primary Cardholder is responsible for use of the Card.

A copy of the law or regulation permitting the issuance of any Prepaid Card Program Youth Card, or an opinion of legal counsel that issuance of a Youth Card is not prohibited by law or regulation, must be provided with the Prepaid Program Registration. If the law or regulation is not in English, then an English translation must also be provided.

An Issuer of a Youth Card may restrict use of the Card by card acceptor business code (MCC), including cash access restrictions. Refer to the *Prepaid Product Constructs* and *Selective Authorization Communications Policy* available on Mastercard Connect™ for additional information and requirements.

6.9.1 Solicitation and Disclosure Requirements

Prior to use, an Issuer must submit all Youth Card Program communications and marketing materials for any Prepaid Card Program including, but not limited to, printed materials and copies or electronic versions of websites and mobile applications, advertisements, card carriers, press releases, websites, welcome letters, marketing plans such as product announcements and program advertisements, consumer applications, and terms and conditions, if any, to the Corporation for review and may not use any such materials without the express approval of the Corporation.

6.10 Prepaid Card Programs

A Mastercard, Maestro, or Cirrus Card Program may be issued as a Prepaid Card Program.

A Prepaid Card Program means:

1. An Account that accesses value maintained by an Issuer or a third party designated by the Issuer on behalf of the owner of the funds in the Account, the value of which shall be fully available to the owner of the funds in the Account at all times; or
2. Any other permitted form of Electronic Money.

Typically, and by regulatory requirement in some markets, the funds are maintained in an omnibus, segregated trust, or pooled account.

6.10.1 Prior Consent of the Corporation

A Customer must not conduct or modify an existing Prepaid Card Program without the express prior consent of the Corporation.

Each Customer request to conduct or modify a Prepaid Card Program must be submitted to, and approved by, the Corporation using the Prepaid Program Registration process available on Mastercard Connect™.

NOTE: A Mastercard® Prepaid Health Savings Account Program is excluded from Prepaid Program Registration. Refer to the *Prepaid Product Constructs* and the *Selective Authorization Communications Policy* available on Mastercard Connect™ for specific Prepaid Card Program information.

6.10.2 Reservation of Rights

The Corporation reserves the right:

1. To approve or reject any Prepaid Card Program application; and
2. To require that any previously approved Prepaid Card Program be modified and/or updated on a recurring basis; and
3. To withdraw its approval of any Prepaid Card Program and require the Prepaid Card Program to be terminated. A Customer may request that the Chief Franchise Officer of the Corporation review the rejection or withdrawal of the approval of a Prepaid Card Program. Such a request must be submitted in writing and signed by the Customer's principal contact. The request must be postmarked no later than 30 days after the date of receipt of the notice of rejection or withdrawal of approval. Any decision by the Chief Franchise Officer with respect to such rejection or withdrawal of approval is final and not subject to further review or other action.

6.10.3 Responsibility for the Prepaid Card Program

An Issuer is responsible for its Prepaid Card Programs, the Prepaid Card Program funds associated with those Prepaid Card Programs, and for the actions (or inaction) of any agents it uses in connection with such Prepaid Card Programs.

The Corporation exclusively determines if an Issuer is in compliance with the foregoing requirements.

6.10.4 Categories of Prepaid Card Program

The Corporation categorizes Prepaid Card Programs into three categories: consumer, commercial, and government.

The Corporation may adopt additional and/or review the current categories of Prepaid Card Programs from time to time in its sole discretion.

Consumer Prepaid Card Programs

Consumer Prepaid Card Programs are Prepaid Card Programs in which the funds may be deposited in the prepaid Account by the consumer, a commercial entity and/or a government entity.

In the case of Consumer Prepaid Card Programs, the funds deposited in the prepaid Account are owned by the consumer.

Commercial Prepaid Card Programs

Commercial Prepaid Card Programs are Prepaid Card Programs in which the funds are deposited in the prepaid Account by a commercial entity.

In the case of Commercial Prepaid Card Programs, the funds deposited in the prepaid Account may be owned by the commercial entity or by the consumer or other third party designated by the commercial entity or such consumer. If the commercial entity permits a consumer to deposit funds in the prepaid Account owned by the commercial entity, the Commercial Prepaid Card Program becomes a Consumer Prepaid Card Program and all relevant Consumer Prepaid Card Program requirements apply.

Government Prepaid Card Programs

Government Prepaid Card Programs are Prepaid Card Programs in which the funds are deposited in the prepaid Account by a government entity.

Government Prepaid Card Programs are designed to deliver government payments to a person, including, but not limited to, segmented non-taxable wages, social benefits, pensions and emergency assistance, as governed by applicable law.

In the case of Government Prepaid Card Programs, the funds deposited in the prepaid Account may be owned by the government entity or by the consumer or other third party designated by the government entity or such consumer. If the government entity permits a consumer to deposit funds in the prepaid Account owned by the government entity, the Government Prepaid Card Program becomes a Consumer Prepaid Card Program and all relevant Consumer Prepaid Card Program requirements apply.

6.10.5 Return of Unspent Value

The Issuer must return any unspent funds in the prepaid Account to the owner of that Account in compliance with applicable law or regulation.

In instances where applicable law or regulation does not provide time frames concerning the return of unspent funds, the Issuer must comply with the requirements set forth in this Rule. Subject to applicable law or regulation, an Issuer has no obligation to return unspent funds in

the prepaid Account if the identity of the owner of the unspent funds has not been provided to the Issuer.

Consumer Prepaid Card Programs

An Issuer of Consumer Prepaid Card Programs must provide the consumer with a minimum of 12 months from the date of the last value load or 30 days after the expiration date, whichever comes later, to request the return of unspent funds, less any applicable fees imposed by the Issuer or any other lawful offsets.

Prominent disclosure must be made to the consumer as to how and when to request the refund of unspent funds and as to any fees that apply to the Prepaid Card Program.

Once the consumer submits a refund request, the consumer must receive a refund of unspent funds within 30 days of the date on which the refund request was received by the Issuer.

Commercial Prepaid Card Programs

The Issuer of a Commercial Prepaid Card Program must provide the commercial entity or individual or other third party designated by the commercial entity or consumer with a minimum of 30 days, or as otherwise approved by the Corporation, to spend the funds in the prepaid Account, after which time the funds may revert to the commercial entity or, as otherwise agreed between the commercial entity and the Issuer or its agents (if any), to the Issuer or its agents.

Government Prepaid Card Programs

If the owner of the funds in the prepaid Account is a government entity, then the Issuer of the Government Prepaid Card Program must provide the government entity with a minimum of 30 days, or as otherwise approved by the Corporation, to spend the funds in the prepaid Account, after which time the funds may revert to the government entity or, as otherwise agreed between the government entity and the Issuer or it agents (if any), to the Issuer or its agents.

If the owner of the funds in the prepaid Account is a consumer, then the Issuer of the Government Prepaid Card Program must provide the consumer with a minimum of 12 months from the date of the last value load or 30 days after the expiration date, whichever comes later, to request the return of unspent funds, less any applicable fees imposed by the Issuer or any other lawful offsets. Prominent disclosure must be made to the consumer as to how and when to request the refund of unspent funds and as to any fees that apply to the Prepaid Card Program.

Once the consumer submits a refund request, the consumer must receive a refund of unspent funds within 30 days of the date on which the refund request was received by the Issuer.

6.10.6 Value Loading

Subject to the restrictions set forth below, the maximum load value and load parameters associated with a prepaid Account are established by the Issuer of the Prepaid Card Program and are subject to review and approval by the Corporation.

For Consumer or Commercial Prepaid Card Programs, the Corporation permits a maximum load value per day of USD 5000, EUR 4000, GBP 3500, or for all other currency types, the local

currency equivalent of USD 5000. If an Issuer needs to increase the above-referenced maximum daily amount or otherwise structure the loading of funds into the prepaid Account, the Corporation will evaluate the proposed Prepaid Card Program on a case-by-case basis. However, funds deposited into the prepaid Account via Automatic Clearing House (ACH), Bankers' Automated Clearing Services (BACS), Clearing House Automated Payment System (CHAPS), or any other electronically transferred payroll payments may exceed the above-referenced maximum daily amount.

The Corporation reserves the right to reduce the maximum amount described above in certain circumstances and/or in connection with certain Prepaid Card Programs.

NOTE: Modifications to this Rule appear in the "Canada Region," "Middle East/Africa Region," and "United States Region" chapters.

6.10.7 Automatic Value Loads from Payment Cards

A payment card must not be used to automatically fund a purchase Transaction effected with a prepaid Account, except pursuant to an automatic value load or "top-up" arrangement agreed in advance by the Cardholder pursuant to predefined fixed parameters. For example, an automatic top-up may occur:

- In a predefined amount on a periodic time-based schedule, such as daily, weekly, or monthly; or
- In a predefined amount whenever a certain Account balance is reached (for example, a USD 50 top-up is initiated when the Account balance reaches USD 10). Any such predefined amount must not be increased at the time of authorization.

If an automatic top-up has occurred and the Account balance remains insufficient to fund a purchase Transaction, then the Issuer must respond to the authorization request with either a partial approval or a decline.

Notwithstanding this Rule, a Prepaid Account may be funded at any time with value accessed from another account maintained by the same Issuer or its designated agent for or on behalf of the same Cardholder.

NOTE: As used in this Rule, "Prepaid Account" means a Mastercard, Maestro, or Cirrus Account issued under a Prepaid Card Program.

6.10.8 Communication and Marketing Materials

If an Issuer's prepaid Cards are intended to be used by Cardholders for personal, family or household use, then the Issuer must provide Cardholders with the terms and conditions of the Prepaid Card Program on or before any purchase is made or activation fees are incurred.

If the Issuer's prepaid Cards are intended to be used by Cardholder for business use, then the Issuer must provide the commercial entity or government entity with the terms and conditions of the Prepaid Card Program on or before any purchase is made or activation fees are incurred.

Thereafter, the Issuer must provide the respective Cardholder, commercial entity or government entity with any amendment or modifications thereto and, in particular, make clear and

conspicuous disclosures with respect to all fees to be incurred by the prepaid Account holder to obtain, use, reload, maintain and/or cash out the balance in the prepaid Account or for any other use, as required by the Standards and applicable law.

Press releases must be submitted for review and approval to the Corporation prior to the launch or subsequent modification of any Prepaid Card Program and prior to any marketing of the Prepaid Card Program.

Upon request, an Issuer must submit all communications and marketing materials including, but not limited to, printed materials and copies or electronic versions of websites and mobile applications, card carriers, websites, welcome letters, consumer applications, and terms and conditions if any, for all Prepaid Card Programs to the Corporation for review and approval prior to the launch or subsequent modification of the Prepaid Card Program and prior to any marketing of the Prepaid Card Program. The Corporation review is limited to compliance with the Standards for Issuer communications. Each Issuer is responsible for ensuring that its Prepaid Card Program communication and marketing materials comply with applicable law and the Standards.

An Issuer of prepaid Cards intended to be used by Cardholders for personal, family or household use must inform Cardholders that, in the event that the available amount in the prepaid Account is less than the purchase amount, some Merchants may not allow the Cardholder to combine multiple payment types (such as cash, check or another payment card) to complete the Transaction. Issuers of prepaid Cards intended to be used by Cardholders for business use must inform the commercial entity or government entity of the foregoing.

An Issuer of prepaid Cards intended to be used by Cardholders for personal, family or household use must inform Cardholders if their prepaid Cards are linked to a selective authorization Program. Issuers of prepaid Cards intended to be used by Cardholders for business use must inform the commercial entity or government entity of the foregoing. Refer to the *Prepaid Product Constructs* and *Selective Authorization Communications Policy* available on Mastercard Connect™ for additional information.

6.10.9 Anonymous Prepaid Card Programs

Prepaid Card Programs for which the Issuer does not collect, store or otherwise validate the consumer's identity are subject to the *Guidelines for Anonymous Prepaid Card Programs*, available on Mastercard Connect™.

6.10.10 BINs

An Issuer must use a dedicated BINs/IINs and associated prepaid product codes in conjunction with its Prepaid Card Programs.

In the event of dispute or uncertainty, the Corporation determines, in its sole discretion, BINs/IINs and associated prepaid product codes in conjunction with an Issuer's Prepaid Card Programs.

6.10.11 Simplified Due Diligence Guidelines

NOTE: A Rule on this subject appears in the "Europe Region" chapter.

6.10.12 Debit Mastercard Meal/Food Voucher Card Program

NOTE: A Rule on this subject appears in the "Europe Region" chapter.

6.11 Maestro Chip-only Card Programs—Europe Region Only

NOTE: A Rule on this subject appears in the "Europe Region" chapter.

6.12 Debit Card Programs Issued by Electronic Money Institutions and Payment Institutions

NOTE: A Rule on this subject appears in the "Europe Region" chapter.

6.13 Decoupled Payment Card Programs

NOTE: A Rule on this subject appears in the "Europe Region" chapter.

Chapter 7 Service Providers and Network Enablement Partners

This chapter contains Rules that apply to Customers that use Service Providers for the performance of Program Service and to Network Enablement Partners.

7.1 Service Provider Categories and Descriptions

A Service Provider is categorized by the Corporation based upon the Corporation's understanding of the nature of the Program Services to be performed, as described below (the "Program Service(s)").

A Service Provider may only perform the Program Services such Service Provider is registered by the Customer to perform.

A corporate affiliate of a Customer that is Owned or Controlled by the Customer or by the Customer's ultimate parent and which performs Program Service exclusively for the Customer and not for any other Customer is deemed not to be a Service Provider.

Category / Program Service Name	Description	List of Services
3-D Secure Service Provider (3-DSSP) / 3-D Secure Program Service	A 3-D Secure Service Provider adheres to the 3-D Secure protocol that is designed to offer an additional layer of security for online transactions. The protocol provides an authentication step prior to authorization. Authentication is based on the three-domain model that includes domains for the Issuer, Acquirer, and interoperability. The Corporation operates within the interoperability layer using the Corporation's Directory Server (DS) that routes all 3-D Secure-enabled Mastercard traffic to the appropriate Merchant and Issuer solutions for Cardholder authentication.	• Operates a 3-D Secure Server (3- DSS) system that facilitates communication, via the EMV 3-D Secure specification, to initiate Cardholder authentication under the Mastercard Identity Check Program rules • Operates an Access Control Server (ACS) system that verifies, using the EMV 3-D Secure specification, whether authentication is available for a Card number and device type, and authenticates specific Cardholders under the Mastercard Identity Check Program rules
AML/Sanctions Service Provider / AML/Sanctions Program Service	Provides services related to Anti-Money Laundering (AML) compliance and/or sanctions activities (excluding technical solutions providers)	• AML compliance, including but not limited to KYC, CDD/EDD, and AML transaction monitoring • Sanctions/watchlist screening activities

Category / Program Service Name	Description	List of Services
Data Storage Entity (DSE)/DSE Program Service	Provides any service affording access to Account, Transaction, PTA Account, and/or PTA Transaction data and not identified by the Corporation as TPP Program Service or Payment Facilitator Program Service	• Merchant website hosting or other service involving the computer-based storage of Account, Transaction, PTA Account, or PTA Transaction data • External hosting or provision of payment applications, such as website shopping carts • Encryption key loading • Any other service determined by the Corporation in the Corporation's sole discretion to be DSE Program Service
Digital Activity Service Provider (DASP) / DASP Program Service	Provides provisioning and Token Requestor service	• Provisioning and Token Requestor services with Mastercard Digital Enablement Service (MDES) on behalf of an Issuer • Provisioning services with MDES on behalf of a Token Requestor • Any other service specified by the Corporation in the Corporation's discretion from time to time to be DASP Program Service
Dynamic Currency Conversion Service Provider (DCC Service Provider) / DCC Program Service	Provides POI currency conversion or dynamic currency conversion (DCC)	POI currency conversion or dynamic currency conversion (DCC)

Category / Program Service Name	Description	List of Services
Independent Sales Organization (ISO) / ISO Program Service	Provides Cardholder, Merchant, and/or Account Holder Solicitation, including application processing	• Cardholder, Merchant, and/or Account Holder customer service not affording access to Account data, Transaction data, Payment Transfer Activity (PTA) Account data, and/or PTA Transaction data, including the collection of any fee or other obligation associated with the Customer's Program • Cardholder, Merchant, and/or Account Holder statement preparation not affording access to Account, Transaction, Account Holder, or PTA Transaction data • Merchant education and training • Terminal deployment, not including ATM Terminal deployment by an ATM Terminal owner that does not perform any other type of ISO Program Service • Any other service determined by the Corporation in the Corporation's sole discretion to be ISO Program Service

Category / Program Service Name	Description	List of Services
Installment Service Provider/ Installment Program Service	Provides installment lending services to Issuers related to installment lending activity. Such services may include providing an End User with a loan for purchase of goods and services.	• Enters into an Installment Lending Agreement with an End User that governs the terms of repayment of installment debt by the End User for the purchase of goods and services • Distributes to an End User an Account for purposes of completing the payment stage of a Transaction between the End User and a retailer covered by the Installment Lending Agreement • Submits to the Issuer records of valid Transactions conducted pursuant to the Program Service agreement • Provides an installment technology platform hosting the installment lending account and/or performs installment account management services to Issuers, which may include End User customer service, installment lending authorization services, installment clearing services, installment settlement processing, installment account statement preparation, installment dispute management, and installment fraud screening • Any other service determined by the Corporation in its sole discretion to be Installment Program Service

Category / Program Service Name	Description	List of Services
Merchant Monitoring Service Provider (MMSP)/MMSP Program Service	Provides Merchant website URL content monitoring	• Merchant website URL content monitoring, including monitoring Merchant Activity and Merchant website URLs to determine compliance with the Standards pertaining to the Merchant Monitoring Program • Detection of Transaction laundering and the monitoring of related activity whereby a Merchant or Submerchant processes Transactions on behalf of another Merchant or Submerchant with whom the Acquirer or the Acquirer's Payment Facilitator does not have a Merchant Agreement or Submerchant Agreement • Transaction laundering is also factoring or Transaction aggregation • Detection of unauthorized Transaction activity, which may include but is not limited to Transactions that are not authorized by the Cardholder or that arise from business that is not bona fide or was not fully disclosed to the Acquirer or Payment Facilitator, as applicable
Staged Digital Wallet Operator (SDWO) / SDWO Program Service	Provides consumers with a Staged Digital Wallet	• Operates and offers to consumers a Staged Digital Wallet • A Payment Facilitator cannot be a Payment Facilitator for a Staged Digital Wallet

Category / Program Service Name	Description	List of Services
Token Service Provider (TSP)/TSP Program Service	Operates a Token Vault	• Token generation and issuance • Cardholder or Account Holder authentication and token activation • Any other service specified by the Corporation in the Corporation's discretion from time to time to be TSP Program Service
Merchant servicers which are categorized as follows:		
• Payment Facilitator (PF)/PF Program Service	Submits and provides services to Acquirers related to Submerchant activity	• Enters into a Submerchant Agreement as an agent of an Acquirer with each Merchant, including as required in Rule 7.8.1 • Submit to the Acquirer records of valid Transactions submitted to the Payment Facilitator by a Submerchant • Timely pay Submerchants for Transactions submitted to the Payment Facilitator by the Submerchant
• Merchant Payment Gateway (MPG) / MPG Program Service	Provides payment processing services to Merchants including interfacing with Acquirers	• Provides technology that captures and sends payment Transaction data to an Acquirer on behalf of a Merchant, whether in a card-present environment or in a card-not-present environment • Acts as the interface between an e-commerce Merchant Location (e.g., website or mobile app) and the Merchant's Acquirer

Category / Program Service Name	Description	List of Services
• Terminal Servicer (TS) / TS Program Service	Merchant servicer that provides services related to any electronically centralized method of administering Terminal software service (such as, by way of example and not limitation, service performed by remote access to a Terminal)	• Terminal maintenance and support • Technology deployment allowing any method of Terminal Transaction, including a Transaction using a mobile wallet application • Terminal software system operation • Services to support payment terminal compliance relating to the Payment Card Industry Data Security Standard (PCI DSS) • Any other service determined by the Corporation in the Corporation's sole discretion to be TS Program Service
Sponsored Program Managers (SPM) / SPM Program Service	Holds the relationship with the Cardholder or PTA Account Holder, has autonomy over a Card issuing Program or otherwise uses a Corporation Asset	• Coordinates the delivery of a Card Program on behalf of a third-party entity, including engaging with BIN sponsors, processors, and card manufacturers • Provides the operational relationship or otherwise holds the relationship with the Cardholder or PTA Account Holder • Has autonomy over a Card issuing Program • Utilizes any Corporation Assets

Category / Program Service Name	Description	List of Services
Third Party Processor (TPP) / TPP Program Service	Provides Transaction or Cardholder processing services	• Provides service support for mobile remote payment functionality, which is initiated by an enrolled Cardholder from a Cardholder-controlled mobile phone registered with the Issuer, and used for entry of a Cardholder's PIN or mobile-specific credentials • Authorization services, including but not limited to authorization routing, and switching services, voice authorization, and call referral processing • Clearing file preparation and submission • Settlement processing (excluding possession, ownership, or control of settlement funds, which is not permitted) • Cardholder, Merchant, and/or Account Holder statement preparation affording access to Account data, Transaction data, PTA Account data, and/or PTA Transaction data • Cardholder and/or Account Holder customer service affording access to Account data, Transaction data, PTA Account data, and/or PTA Transaction data • Integration with the applicable Corporation Systems for the purpose of origination or reception of PTA Transactions • Fraud control and risk monitoring, including but not limited to fraud screening and fraud scoring services • Chargeback processing for Acquirers or Issuers

Category / Program Service Name	Description	List of Services
		• Chargeback processing for Merchants or Submerchants • Any other service determined by the Corporation in the Corporation's sole discretion to be TPP Program Service **NOTE: Modifications to this Rule appear in the "Europe Region" chapter.**
TPPs / TPP Program Services are subcategorized as follows.		
Type I		• The Corporation determines, in the Corporation's sole discretion, if a TPP is a Type I TPP. Type I TPPs generally are those that perform Program Service for a large number of Customers or that otherwise could significantly impact the integrity of the Interchange System. • A Type I TPP must not also provide ISO Program Service unless registered to provide ISO Program Service. In the Europe Region, Service Providers are no longer designated as Type I TPPs. Any existing Type I TPP may remain as a Type I TPP.
Type II		A Type II TPP is any TPP that the Corporation does not deem to be a Type I TPP. The Corporation at any time may reclassify a Type II TPP as a Type I TPP.
Type III		**NOTE: A Rule on this subject appears in the "United States Region" chapter.**

7.2 The Program Service and Performance of Program Service

Before an entity commences to perform Program Service that supports or benefits a Customer's Program, the Customer must:

- Verify that the entity is operating a bona fide business, has sufficient safeguards in place to protect Account, Transaction, PTA Account, and PTA Transaction data from unauthorized disclosure or use, and complies with applicable laws; and conduct appropriate due diligence to confirm such operations, safeguards and compliance;
- Prior to registering a DASP and TSP confirm that such entity satisfies all certification and testing procedures established by the Corporation before such entity may be registered by a Customer as the Customer's DASP or TSP; and
- Cause such an entity to be registered by the Corporation as a Service Provider.

A Service Provider may perform only the type of Program Service for a Customer that is registered by such Customer to perform.

The Customer must ensure that an entity performing Program Service that supports or benefits the Customer's Program, and whether or not such entity is registered by the Corporation as a Service Provider:

1. Complies with all Standards applicable to the Program Service provided (including, by way of example and not limitation, these Service Provider Rules, data use and protection, confidentiality and privacy Standards) for so long as such entity performs such Program Service. This Customer obligation arises and continues regardless of the nature of the Program Service performed and whether the entity is performing Program Service pursuant to an agreement or other arrangement with the Customer, a Service Provider of the Customer, or any other entity.
2. Promptly provides to the Corporation any information requested by the Corporation pertaining to the Program Service or the performance thereof.

Program Service in support of or benefiting an Affiliate Program is deemed to be Program Service in support of or benefiting the Program of the Principal that Sponsors such Affiliate. An Affiliate wishing to receive Program Service from a Service Provider must obtain the prior written consent of the Affiliate's Sponsoring Principal.

NOTE: Modifications to this Rule appear in the "Canada Region" chapter.

7.2.1 Customer Responsibility and Control

The Customer must at all times be entirely responsible for and must manage, direct, and control all aspects of the Customer's Program and Program Service performed by Service Providers, and establish and enforce all Program management and operating policies in accordance with the Standards.

A Customer must not transfer or assign any part of such responsibilities or in any way limit such Customer's responsibility with regard to any of such Customer's Service Providers. A Customer

must conduct meaningful monitoring of such Customer's Service Providers to ensure ongoing compliance by such Customer's Service Providers with the Standards.

7.2.2 Notification to the Corporation of Change of Name or Transfer of Ownership or Control

Each Customer must advise the Corporation promptly in writing when any of such Customer's Service Providers.

1. Undergoes a change of name or transfer of Ownership or Control;
2. Fails or refuses to make payments in the ordinary course of business;
3. Makes an assignment for the benefit of creditors; or
4. Seeks bankruptcy protection or similar protection.

A Customer must not receive Program Service by or from any other entity or person except as set forth in the Standards.

NOTE: Modifications to this Rule appear in the "United States Region" chapter.

7.2.3 Program Service Agreement

This Rule is not applicable with respect to a Service Provider whose provision of Program Service to the Customer consists only of DSE Program Service, DWO Program Service, DASP Program Service, MMSP Program Service, TS Program Service, or 3-D Secure Program Service.

Prior to the commencement of the performance of Program Service by an entity in support of a Customer Program, the Customer and the Service Provider must enter into a written agreement describing the Program Service to be performed (the "Program Service agreement"). The Program Service agreement must be updated from time to time as appropriate to reflect the Program Service that the Service Provider performs in support of or benefiting, the Customer Program and must be consistent with the Standards.

The Program Service agreement must reflect the Customer's responsibility for establishing all management and operating policies described in the Standards and must not include any provision that attempts to limit the Customer's responsibility for the Program. The Program Service agreement must include all of the following provisions:

1. The Service Provider received, understands, and agrees to comply with all applicable Standards, including the Service Provider Rules.
2. On an ongoing basis, the Service Provider is promptly to provide the Customer with the current addresses of each of such Service Provider's offices.
3. In the event of any inconsistency between any provision of the Program Service agreement and the Standards, the Standards govern.
4. The Program Service agreement automatically and immediately terminates if the Corporation de-registers the Service Provider or if the Customer ceases to be a Customer or if the Customer fails to have a valid License by the Corporation to use any Mark pertaining to the Program Service to be performed by the Service Provider.

5. The Service Provider acknowledges that the Corporation is the sole owner of the Marks, agrees not to contest the ownership of the Marks for any reason, and agrees the Corporation may prohibit the Service Provider from using any of the Marks for any reason.
6. The Service Provider acknowledges that the Corporation has the right to enforce any provision of the Standards and to prohibit a Service Provider from engaging in any conduct the Corporation deems could create a risk of injury to the Corporation, or that could adversely affect the integrity of the Interchange System, and agrees not to take any action that could interfere with the exercise of this right by the Corporation.

7.2.4 Disclosure of Standards

Before a Customer proposes an entity to be registered as a Service Provider by the Corporation, the Customer must provide or ensure the proposed Service Provider has access to the Standards then in effect applicable to Service Providers and Program Service the proposed Service Provider is expected to perform.

After registration, the Customer must provide, or ensure a Service Provider is notified of, any change to the Standards applicable to such Program Service.

7.2.5 Customer Point of Contact

A Service Provider must promptly provide a name and title of, and a telephone number for an employee of the Customer upon request by a Cardholder, Account Holder, or an ATM owner, or if the Service Provider is unable or unwilling to respond to a question to the Cardholder's, Account Holder's, or ATM owner's satisfaction.

7.2.6 Use of the Marks

A Service Provider must not use any Mark on such Service Provider's own behalf, whether in connection with Program Service or otherwise.

The Service Provider must not create an impression that the Service Provider is a Customer or a representative of the Corporation.

A Service Provider must not create an impression that the Corporation in any way endorses the Service Provider or the Program Service that the Service Provider performs.

A Service Provider may use one or more of the Marks in connection with the Program Service such Service Provider performs, provided:

1. The Marks are used in accordance with the Standards, including all current reproduction, usage and artwork Standards; and
2. The Marks are used according to the express written instructions of the Customer; and
3. The Marks are used solely in connection with the provision of Program Service. The Service Provider may use the Marks on such Service Provider stationery, letterhead, or business cards only if accompanied, in close proximity, by a clear statement that identifies the Service Provider as an agent for a Customer and that includes the name by which the Customer identifies itself to the public (for example, "Service Provider is an authorized representative of Bank XYZ").

7.2.7 Service Provider Identification on a Card

The name of a non-Customer Service Provider may appear on a Card only if that Service Provider does not perform acquiring Program Service in connection with any Customer Program.

7.2.8 Program Materials

A Customer must approve all Program documents before distribution by a Service Provider.

The Program materials must not imply that the Service Provider is participating in any activity not permitted by the Standards. Program materials include, by way of example, Card or Account Holder applications, ATM Owner Agreements, Cardholder or Account Holder agreements, Cardholder or Account Holder statements, marketing materials, and Cardholder or Account Holder Communications, including Solicitations.

7.2.9 Notification of Settlement Failure Obligation

A Service Provider that becomes aware of a settlement failure by the Customers for which the Service Provider performs Program Service must promptly, and in no event later than 24 hours after becoming aware of such failure, notify the Corporation in writing of such failure.

7.2.10 Data Security

A Service Provider must comply with all Standards pertaining to the storage, safeguarding, and/or transmission of Account, Cardholder, Transaction, PTA Account, Account Holder and PTA Transaction data.

If a Service Provider reasonably believes that an unauthorized person accessed or may have accessed Account, Cardholder, Transaction, PTA Account, Account Holder, or PTA Transaction data in the possession or control of the Service Provider or any other third party, the Service Provider must promptly notify each Customer for which such Service Provider provides Program Service in writing of such belief and the Customer must promptly notify the Corporation in writing of such belief.

The obligations set forth in this Rule survive the termination or expiration of the Program Service agreement.

7.3 Access to Merchant Account

A Service Provider must not have access to any account for funds due to a Merchant or withheld from a Merchant for chargebacks, with the exception of Payment Facilitators, as set forth in Rule 7.8.2.

A Customer must not assign or transfer to a Service Provider an obligation to pay or reimburse a Merchant if the obligation arises from Activity.

7.4 Transfer of Rights Prohibited

A Service Provider must not subcontract, sublicense, assign, license, franchise, or in any other manner extend or transfer to any third party any right or obligation the Service Provider may have in connection with providing Program Service for a Customer, and any such transfer is null and void *ab initio*.

A Service Provider may perform Program Service for a Customer only using the Service Provider's own employees or employees of a different Service Provider that is confirmed also to be registered by the Corporation to perform Program Service for that same Customer.

7.5 Use of Corporation's Systems and Confidential Information

For purposes of this Rule, "the Corporation's Systems" means any of the Corporation's equipment and software and "the Corporation's Confidential Information" means any of the Corporation's information identified or reasonably understood to be confidential or proprietary.

A Service Provider performing Program Service must agree to:

1. Use any of the Corporation's Systems, including but not limited to any Mastercard Interface Processor (MIP) or Network Interface Processor (NIU) used to connect to the Interchange System, and any of the Corporation's Confidential Information solely in order to perform Program Service on behalf of the Customer;
2. Treat the Corporation's Systems and Confidential Information in at least as careful and confidential a manner as the Service Provider treats such Service Provider's own and the Customer's systems and proprietary information;
3. Acknowledge that access to the Corporation's Systems and Confidential Information does not provide the Service Provider with any right to use them further;
4. Limit access to the Corporation's Systems and Confidential Information to those Service Provider employees with a need to have access in order to enable the Service Provider to perform Program Service and to implement and to maintain reasonable and appropriate safeguards to prevent unauthorized access to the Corporation's Systems or disclosure of the Corporation's Confidential Information, including those set forth in section 1.4, "Connecting to Mastercard—Physical and Logical Security Requirements," of the *Security Rules and Procedures* manual;
5. Immediately cease any use of the Corporation's Systems and Confidential Information upon request of the Corporation or the Customer or upon the earlier of the termination or completion of the Service Provider's performance of Program Service, and to immediately deliver all of the Corporation's Systems and Confidential Information to the Corporation; and
6. Immediately advise the Customer and the Corporation if any unauthorized person seeks to gain or gains access to the Corporation's Systems or Confidential Information, whether by legal proceedings or otherwise.

The obligations set forth in this Rule survive the termination or expiration of the Program Service agreement.

7.6 Acquiring Programs

Each Acquirer and each Service Provider that performs Program Service with respect to that Acquirer's acquiring Programs must comply with all of the following.

7.6.1 Merchant Agreement

The Merchant Agreement establishing the terms of an acquiring relationship between the Acquirer and a Merchant must:

1. Be signed by the Acquirer with no separate or other agreement between the Service Provider and the Merchant regarding Activity. The Service Provider may be a party to the Merchant Agreement, in which case the Merchant Agreement must contain the substance of all of the following:
   a. For purposes of the Merchant Agreement and performance of the Merchant Agreement by the Service Provider, (i) the Service Provider is the exclusive agent of the Acquirer; (ii) the Acquirer is entirely responsible for, and in control of, Service Provider performance; and (iii) the Acquirer must approve, in advance, any fee payable to or obligation of the Merchant arising from or related to performance of the Merchant Agreement.
   b. The Merchant Agreement is not effective and must not be modified in any respect without the express written agreement of the Acquirer.
   c. The Service Provider must not have access, directly or indirectly, to any account for funds or funds due to a Merchant and/or funds withheld from a Merchant for chargebacks arising from, or related to, performance of this Merchant Agreement. The Acquirer may not assign or otherwise transfer an obligation to pay or reimburse a Merchant arising from, or related to, performance of the Merchant Agreement to a Service Provider.
   d. The Service Provider must not subcontract, sublicense, assign, license, franchise, or in any manner extend or transfer to any third party, any right or obligation of the Service Provider set forth in the Merchant Agreement. The Acquirer must not waive, forgive, release, assign, or fail to insist on strict performance of each requirement set forth in these parts 1 through 4.
2. Confirm the Acquirer's responsibility for the Program and for the Merchant's Program participation and confirm that the Merchant Agreement does not contain any provision that could be deemed to limit such responsibility.
3. Not take effect or state or imply that such Merchant Agreement takes or has taken effect prior to being signed by the Acquirer.
4. Disclose the Acquirer's name and sufficient information to enable the Merchant to contact the Acquirer directly by telephone or in writing.

7.6.2 Collection of Funds from a Merchant or ATM Owner

Discount rates (or similar charges called by other terms) due to an Acquirer from a Merchant or ATM Owner must be collected directly by the Acquirer and not by a Service Provider.

7.6.3 Access to Documentation

The Acquirer at all times must maintain prompt and unrestricted physical access to all original, executed Merchant Agreements and ATM Owner Agreements and to completed Merchant and ATM site inspection reports.

The Acquirer must forward true and complete copies of any one or more of these documents to the Corporation promptly upon request.

7.6.4 Authority to Terminate Merchant Agreement or ATM Owner Agreement

An Acquirer must not limit or in any manner condition such Acquirer's authority to terminate any Merchant Agreement or ATM Owner Agreement to accommodate a Service Provider or otherwise.

7.6.5 Payment Facilitators and Submerchants

The Acquirer is responsible for all acts and omissions of a Payment Facilitator and of any Submerchant and is responsible for ensuring that each Payment Facilitator and Submerchant complies on an ongoing basis with all Standards applicable to Merchants.

NOTE: Modifications to this Rule appear in the "United States Region" chapter.

7.6.5.1 Responsibility for Payment Facilitator and Submerchant Activity

The Acquirer must ensure ongoing compliance with all of the following.

1. A Submerchant of a Payment Facilitator must be located within the Acquirer's Area of Use as described in Rule 1.7. The Acquirer must obtain an extension of such Acquirer's Area of Use if the Submerchant is located elsewhere, except as provided in Rule 1.7.2 paragraph 6. The location of the Submerchant determines the location of a Transaction, not the location of the Payment Facilitator. A Payment Facilitator may be located outside of the Acquirer's Area of Use.
2. Settlement funds the Acquirer permits a Payment Facilitator to access may only be used to pay Submerchants pursuant to the terms of their Submerchant Agreements.
3. An Acquirer may permit a Payment Facilitator to manage the following obligations on behalf of the Acquirer, and remains fully responsible for the fulfillment of each to the extent that the Payment Facilitator fails to do so:
   a. Verify that a Submerchant is a bona fide business operation, as set forth in section 7.1.1, "Required Screening Procedures" of the *Security Rules and Procedures* manual; and
   b. Retain records concerning the investigation of a prospective Submerchant, provided that such records are provided to the Acquirer immediately upon request; and
   c. Pay a Submerchant for Transactions, in accordance with Rule 7.8.2 part 4; and
   d. Ensure that a Submerchant is supplied with materials necessary to effect Transactions as set forth in Rule 7.8.2 part 5; and

e. Monitor a Submerchant's Activity on an ongoing basis to deter fraud or other wrongful activity, as set forth in Rule 7.8.2, part 6.

4. A Payment Facilitator and a Submerchant must follow the applicable Standards, including Rule 5.12.6 regarding the Cardholder's right to dispute a Transaction.
5. The Acquirer must provide to the Corporation a quarterly Activity report for each Submerchant of the Payment Facilitator that includes:
   a. Submerchant name and location as appears in DE 43 (Card Acceptor Name/Location) of clearing records
   b. Submerchant "doing business as" name or URL;
   c. Submerchant MCCs;
   d. Transaction sales count and amount for each MCC; and
   e. Transaction chargeback count and amount for each MCC.
   The requirements in this part 5 are not applicable to Processed Transactions provided the Acquirer populates Payment Facilitator ID and Submerchant ID data as set forth in Rule 7.6.6, and unless otherwise required by the Corporation.
6. An Acquirer that uses a Payment Facilitator that proposes to sponsor a Submerchant conducting business that may be described under any one of the MCCs listed in section 9.1 of the *Security Rules and Procedures* manual or any entity that, as a Merchant, was reported under the Excessive Chargeback Program, must register such Submerchant in the Mastercard Registration Program (MRP) system using Mastercard Connect™ before accepting Transactions arising from such entity, whether directly or through a Payment Facilitator, as described in Chapter 9 of the *Security Rules and Procedures* manual. The Merchant monitoring requirements set forth in Chapter 9 of the *Security Rules and Procedures* manual apply to Submerchants of Payment Facilitators.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

7.6.6 Transaction Identification for ISO and PF Transactions

An Acquirer that uses:

- an Independent Sales Organization (ISO) must populate the ISO field with an Independent Sales Organization ID; and
- a PF must populate the Payment Facilitator field with a Payment Facilitator ID assigned by the Corporation and the Submerchant field with the unique Submerchant ID assigned by the Payment Facilitator to uniquely identify the Submerchant;

in all Transaction messages arising from a Merchant, Submerchant, or ATM owner receiving or otherwise benefiting from the Program Service performed by that such Service Provider as required by the *Customer Interface Specification*, *IPM Clearing Formats*, and *Single Message System Specifications* manuals.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

7.6.7 Staged Digital Wallet Operator Requirements

The Acquirer is responsible for complying with the following.

1. The Acquirer must notify the Corporation if a Staged DWO enables Transactions with an entity providing goods or services classified under the Card acceptor business codes (MCCs) set forth in section 9.1 of the *Security Rules and Procedures* manual.
2. The Acquirer must process all Staged DWO funding stage Transactions as Card-not-present Transactions.
3. The Acquirer of a Staged DWO must accept liability for any valid chargeback that arises in connection with a Transaction, such as a chargeback arising in connection with a Cardholder's claim that the Cardholder did not register the Mastercard or Maestro Account as a funding account for the Staged Digital Wallet or did not otherwise consent to the use of the Staged Digital Wallet as a payment method. The Acquirer must ensure that the Staged DWO complies with Rule 9.1, and with the following requirements applicable to Staged DWOs:
   a. A Mastercard or Maestro Account must not be used to fund a Transaction that would be in violation of Rule 5.12.7.
   b. The payment stage of a Transaction facilitated by a Staged DWO must not be completed with a Mastercard or Maestro branded Card.
   c. A Staged DWO must not process a Transaction on behalf of another Staged DWO.
   d. The Staged DWO must transmit the three-digit Wallet Identification Number (WID) assigned to the Staged DWO by the Corporation in DE 48, subelement 26, subfield 1 of all Authorization Request/0100 messages and in PDS 0207 of all First Presentment/1240 messages for load Transactions.
   e. The Staged DWO and each retailer receiving payment by means of a Staged DWO payment account must be located within the Acquirer's Area of Use as described in Rule 1.7 (regardless of the form of payment).
   f. The Staged DWO must perform customer service and provide contact information with which the consumer may request the assistance of the Staged DWO in the resolution of any disputes involving a commercial entity that displays the Staged DWO mark.
   g. The Staged DWO must be identified in each funding stage Transaction, defined as a Transaction authorized during an End User's purchase of products or services from a retailer, including but not limited to a Merchant, Submerchant, or other commercial entity, as follows:
      - The Staged DWO name in conjunction with the retailer name in the format "Staged DWO*Retailer"
      - The retailer location address
      - The MCC that most closely describes the retailer's primary business

Refer to the *Mastercard MoneySend and Funding Transactions Program Standards* regarding the identification of Staged Digital Wallet Funding Transactions. An SDWO that is also an Installment Service Provider must identify installment billing Transactions as set forth in section 5.5.2, "Multiple-Authorization Installment Billing" of the *Transaction Processing Rules*.

MCC 6540 must not be used for a funding stage Transaction if such funds may subsequently be used for any of the following purposes; in such event, the funds must be segregated and used by the consumer solely for the designated purpose:

- The purchase of chips or other value usable for gambling (MCC 7801, MCC 7802, or MCC 7995 must be used);
- The purchase of access to adult content and services (MCC 5967 must be used);
- The purchase of any prescription drug (MCC 5122 or MCC 5912 must be used);
- The sale of any tobacco product (MCC 5993 must be used)
- The purchase of high-risk cyberlocker services (MCC 4816 must be used);
- The purchase of high-risk securities (MCC 6211 must be used); or
- The purchase of any cryptocurrency (MCC 6051 must be used).

NOTE: Modifications to certain provisions of this Rule appear in the "Canada Region," "Europe Region," and "United States Region" chapters.

7.7 Issuing Programs

Each Customer and each Service Provider that performs Program Service with respect to that Customer's issuing Programs must comply with all of the following:

7.7.1 Card Application Approval

The Customer itself, and not a Service Provider, must approve the application of a person to participate as a Cardholder in the Customer's Card Program.

7.7.2 Cardholder Agreement

The Cardholder agreement must disclose the Customer's name and sufficient information to enable the Cardholder to contact the Customer directly by telephone or in writing.

The Service Provider must not be a party to the Cardholder agreement.

7.7.3 Program Payments

All Program payments other than Card application fees paid by prospective Cardholders must be collected directly by the Customer and not by the Service Provider.

7.7.4 Program Receivables

A Service Provider may own Program receivables or participate in a financing vehicle involving such receivables so long as the Corporation determines that the Customer continues to own and control the Program.

Ownership of such receivables by the Service Provider does not in any way limit the Customer's obligation to comply with the Standards.

7.7.5 Installment Service Provider Program Requirements

The Issuer is responsible for complying with the following:

1. The Issuer must notify the Corporation if an Installment Service Provider enables Transactions with a retailer classified under the Card acceptor business codes (MCCs) set forth in section 9.1 of the *Security Rules and Procedures* manual.
2. The Issuer for an Installment Service Provider must accept liability for any valid chargeback that arises in connection with a Transaction, such as arising in connection with a Cardholder's claim that they did not register the Mastercard or Maestro Account as a repayment account for the Installment Service Provider or did not otherwise enter into the Installment Lending Agreement.
3. The Issuer for an Installment Service Provider must ensure that Rule 6.2 regarding Issuer disclosures to Cardholders and Rule 6.3 (the "zero liability" Rule) apply to any Transactions conducted pursuant to a Program Service agreement.

The Issuer must ensure that the Installment Service Provider complies with the following requirements applicable to Installment Service Providers:

1. A Mastercard or Maestro Account must not be used at the payment or repayment stage of a Transaction that would be in violation of Rule 5.12.7, which prohibits the submission of illegal or brand-damaging Transactions.
2. An Installment Service Provider must not conduct a Transaction on behalf of another Installment Service Provider.
3. The Installment Service Provider must enter into an Installment Lending Agreement with each End User, and such agreement must provide for a series of payments in accordance with a fixed repayment schedule.
4. The Installment Service Provider must distribute to the End User an Account for the purposes of completing the payment stage of the Transaction between the End User and a retailer covered by the Installment Lending Agreement.
5. The Installment Service Provider and each retailer receiving payment by means of an Account distributed by the Installment Service Provider must be located within the Issuer's Area of Use as described in Rule 1.7 (regardless of the form of payment).
6. The Installment Service Provider must perform customer service and provide contact information with which the End User may request the assistance of the Installment Service Provider in the resolution of any disputes involving an Installment Transaction.

7.8 Payment Facilitator Obligations

The Acquirer must ensure that such Acquirer's Payment Facilitator satisfies all of the obligations set forth in this Rule.

A Payment Facilitator may not be a Submerchant of any other Payment Facilitator, nor may a Payment Facilitator be a Payment Facilitator for another Payment Facilitator. A Payment Facilitator must not be a Payment Facilitator for a Staged Digital Wallet. Unless the Submerchant Threshold Conditions are met, any Submerchant that exceeds USD 10,000,000 in

Mastercard and Maestro combined annual Transaction volume must enter into a Merchant Agreement directly with a Customer.

If all of the conditions set forth in Item 1 or the condition set forth in Item 2 are met (the "Submerchant Threshold Conditions"):

1. Each of:
   - The Payment Facilitator is registered as a Network Enablement Partner;
   - Acquirer's use of Payment Facilitator(s) has undergone a Franchise Management Program review) as described in Chapter 13 of the Security Rules and Procedures manual;
   - The Acquirer has read-only access to the Payment Facilitator's systems;
   - In an e-commerce environment, the Payment Facilitator uses a Merchant monitoring solution to review their e-commerce Submerchants' Activity to confirm compliance with Rule 5.12.7; and
   - The Acquirer reviews at least 5% of the total number of its Payment Facilitator's newly onboarded Submerchants on a monthly basis for compliance with the Acquirer's risk tolerance policies and requirements and for compliance with the Standards;
   Or
2. The MCC that reflects the primary business of the Submerchant is one of the Threshold Exception MCCs;

Then,

A. The Submerchant is not required to enter into a Merchant Agreement directly with a Customer;

B. Settlement funds the Acquirer permits a Payment Facilitator to access may only be used to pay Submerchants pursuant to the terms of their Submerchant Agreements; and

C. The Acquirer may, at the Acquirer's discretion, require a tri-party Submerchant Agreement between the Acquirer, Submerchant and Payment Facilitator.

The "Threshold Exception MCCs" include:

- MCC 4900 (Utilities—Electric, Gas, Heating Oil, Sanitary, Water);
- MCC 6012 (Merchandise and Services—Customer Financial Institution);
- MCC 6513 (Real Estate Agents and Managers – Rentals);
- MCC 8011 (Doctors [Not Elsewhere Classified]);
- MCC 8050 (Nursing and Personal Care Facilities);
- MCC 8062 (Hospitals);
- MCC 8099 (Medical Services and Health Practitioners [Not Elsewhere Classified]);
- MCC 8211 (Schools, Elementary and Secondary);
- MCC 8220 (Colleges, Universities, Professional Schools, and Junior Colleges);
- MCC 8241 (Schools, Correspondence);
- MCC 8244 (Schools, Business and Secretarial);
- MCC 8249 (Schools, Trade and Vocational);

- MCC 8299 (Schools and Educational Services [Not Elsewhere Classified]); and
- MCC 9311 (Tax Payments).

An Acquirer relying on Item 1 of the Submerchant Threshold Conditions may be required to undertake a yearly Franchise Management Review Program of the Acquirer's use of Payment Facilitator(s) as described in Chapter 13 of the *Security Rules and Procedures* manual.

7.8.1 Submerchant Agreement

Pursuant to a written agreement between an Acquirer and a Payment Facilitator, a Payment Facilitator may enter into a Submerchant Agreement with a Submerchant for the purpose of facilitating the Acquirer's acquiring of Transactions from the Submerchant.

The Submerchant Agreement must conform to Standards pertaining to Merchant Agreements, and must clearly and conspicuously reflect that the Payment Facilitator is entering into the Submerchant Agreement on behalf of and as an agent of the Acquirer.

The Submerchant Agreement must not interfere with or lessen the right of the Payment Facilitator, the Acquirer, or the Corporation to terminate the agreement at any time. The Corporation reserves the right to restrict a Payment Facilitator from entering into a Submerchant Agreement based on the business of the entity or other criteria as the Corporation deems appropriate.

7.8.1.1 Required Submerchant Agreement Terms

A Submerchant Agreement must include all provisions required to be included in a Merchant Agreement, in addition to complying with Rule 7.8.1 and this Rule 7.8.1.1.

The failure of the Payment Facilitator to include the substance of any one or more of such Standards in the Submerchant Agreement or the grant of a variance by the Corporation with respect to any one or more such Standards does not relieve an Acquirer from responsibility for chargebacks or compliance related to the Activity of or use of the Marks by the Submerchant.

The Submerchant Agreement must, in substance, include all of the following provisions:

1. On an ongoing basis, the Submerchant is promptly to provide the Payment Facilitator with the current address of each of such Submerchant's offices, all "doing business as" (DBA) names used by the Submerchant, and a complete description of goods sold and services provided.
2. In the event of any inconsistency between any provision of the Submerchant Agreement and the Standards, the Standards will govern.
3. The Payment Facilitator is responsible for the Card acceptance policies and procedures of the Submerchant, and may require any changes to such Submerchant's website or otherwise that such Payment Facilitator deems necessary or appropriate to ensure that the Submerchant remains in compliance with the Standards governing the use of the Marks.
4. The Submerchant Agreement automatically and immediately terminates if the Corporation de-registers the Payment Facilitator or if the Payment Facilitator's Acquirer ceases to be a Customer for any reason or if such Acquirer fails to have a valid License with the Corporation to use any Mark accepted by the Submerchant.

5. The Payment Facilitator may, at such Payment Faclitator's discretion or at the direction of such Payment Facilitator's Acquirer or the Corporation, immediately terminate the Submerchant Agreement for activity deemed to be fraudulent or otherwise wrongful by the Payment Facilitator, such Payment Facilitator's Acquirer, or the Corporation.
6. The Submerchant acknowledges and agrees:
   a. To comply with all applicable Standards, as amended from time to time;
   b. That the Corporation is the sole and exclusive owner of the Marks;
   c. Not to contest the ownership of the Marks for any reason;
   d. The Corporation may at any time, immediately and without advance notice, prohibit the Submerchant from using any of the Marks for any reason;
   e. The Corporation has the right to enforce any provision of the Standards and to prohibit the Submerchant and/or such Submerchant's Payment Facilitator from engaging in any conduct the Corporation deems could injure or could create a risk of injury to the Corporation, including injury to reputation, or that could adversely affect the integrity of the Interchange System, the Corporation's Confidential Information (as defined in Rule 7.5), or both; and
   f. The Submerchant will not take any action that could interfere with or prevent the exercise of this right by the Corporation.

The Submerchant Agreement must not contain any terms that conflict with any Standard.

NOTE: Modifications to this Rule appear in the "United States Region" chapter.

7.8.2 Obligations as Sponsor of Submerchants

A Payment Facilitator must fulfill all of the following obligations with respect to each of such Payment Facilitator's Submerchants.

1. **Submit Valid Transactions**

The Payment Facilitator must submit to such Payment Facilitator's Acquirer records of valid Transactions submitted by a Submerchant and involving a bona fide Cardholder. The Payment Facilitator must not submit to such Payment Facilitator's Acquirer any Transaction that the Payment Facilitator or the Submerchant knows or should have known to be fraudulent or not authorized by the Cardholder, or that either knows or should have known to be authorized by a Cardholder colluding with the Submerchant for a fraudulent purpose. For purposes of this Rule, the Submerchant is deemed to be responsible for the conduct of such Submerchant's employees, agents, and representatives.

2. **Submerchant Compliance with the Standards**

The Payment Facilitator must ensure that each of such Payment Facilitator's Submerchants complies with the Standards applicable to Merchants. The Payment Facilitator must provide recurring education and training to Submerchants to ensure compliance with the Standards.

3. **Maintaining Submerchant Information**

The Payment Facilitator must maintain, on an ongoing basis, the names, addresses, and URLs if applicable of each of such Payment Facilitator's Submerchants. The Acquirer must ensure that

the Payment Facilitator promptly supplies the Corporation with any such information upon request.

4. **Payments to Submerchants**

Each Payment Facilitator must pay each Submerchant for all Transactions the Payment Facilitator submits to such Payment Facilitator's Acquirer on the Submerchant's behalf. This obligation is not discharged with regard to a Transaction until the Submerchant receives payment from the Payment Facilitator, notwithstanding any payment arrangement between the Submerchant and the Payment Facilitator or between the Payment Facilitator and such Payment Facilitator's Acquirer.

A Submerchant Agreement may provide for a Payment Facilitator to withhold amounts for chargeback reserves or similar purposes.

5. **Supplying Materials to Submerchants**

Each Payment Facilitator must regularly ensure that each of such Payment Facilitator's Submerchants is provided with all materials necessary to effect Transactions in accordance with the Standards and to signify Card acceptance.

6. **Submerchant Monitoring**

Each Payment Facilitator must monitor on an ongoing basis the Activity and use of the Marks of each of such Payment Facilitator's Submerchants for the purpose of deterring fraudulent and other wrongful activity and to ensure ongoing compliance with the Standards. For purposes of this Rule, the minimum Merchant monitoring Standards set forth in the *Security Rules and Procedures* manual apply with respect to Submerchants.

7. **Provide Information**

Each Payment Facilitator must ensure that each of such Payment Facilitator's Submerchants is provided with the information specified in Rule 5.4.3.

8. **Direct to Issuer Transactions**

A Payment Facilitator (1) whose Transactions are submitted directly to the Interchange System and (2) whose Acquirer does not have the ability to see such Transactions at the time of submission, must register as a Network Enablement Partner.

NOTE: Modifications to this Rule appear in the "United States Region" chapter.

7.9 Type I TPP Obligations

NOTE: A Rule on this subject appears in the "United States Region" chapter.

7.10 Registration and Validation Requirements for Service Providers

Each Principal and Association, for itself and each of its Sponsored Affiliates, and each Digital Activity Customer must use the My Company Manager application on Mastercard Connect™ to:

1. Register any Service Provider and provide all information and material required by the Corporation in connection with the proposed registration to the My Company Manager application or service_provider@mastercard.com, as applicable, within 30 days of the registration application submission date, except as provided below; and
2. Validate that the Customer understands, meets and validates the Customer's responsibilities when using such Service Provider to perform Program Services, within 30 days of the registration application submission date and once during each calendar year thereafter.

To propose a Service Provider for registration as a Service Provider, the Customer must:

- Be a Customer in good standing with the Corporation, and
- If applicable, meet any and all capital requirements designated by the Corporation.

In the Corporation's sole discretion, the Corporation may approve or reject any application for the registration of a Service Provider, and may decline to renew the registration of a Service Provider.

The following requirements apply to registration of all Service Providers:

1. A Service Provider that performs services involving the storage, transmission, or processing of Cardholder data and/or related sensitive data governed by PCI must demonstrate compliance with all applicable PCI Security Standards in accordance with the Mastercard Site Data Protection (SDP) Program compliance requirements for Service Providers, as set forth in Rule 2.2.3 of the *Security Rules and Procedures* manual. The Customer must instruct the proposed Service Provider to contact the Corporation using email at pcireports@mastercard.com and validate the Customer's compliance with the SDP Program after initial registration. The registration of a proposed Service Provider will not be deemed complete until the Customer's compliance is validated.
   This requirement to demonstrate such compliance applies to TPPs, DSEs, AML/Sanctions Service Providers, Payment Facilitators, Staged DWOs, DASPs, Token Service Providers, Terminal Servicers, 3-D Secure Service Providers, and Installment Service Providers, as well as other Service Providers performing the services described above. For any proposed Service Provider that is not compliant, the Corporation must be provided and must approve a compliance action plan, except that a compliance plan is not acceptable for Type I TPP Service Providers. A Corporation-approved compliance action plan does not exempt the Customer from responsibility and liability that arises from such Customer's or any of such Customer's Sponsored Affiliates' or their Service Provider's noncompliance with any Standard, including those relating to the disclosure and securing of Account, Cardholder, and Transaction data. The registration of a proposed Service Provider that performs such services will not be deemed complete until such Service Provider's compliance is validated.
2. The Customer must receive the Corporation's written confirmation of the registration before using a Service Provider for Program Service.

3. After registration by the Corporation of a Service Provider, an initial registration fee and the applicable annual renewal fee is charged by the Corporation to the Customer and debited from the Customer using MCBS, or in the case of Type I TPP, charged by the Corporation directly to the Type I TPP. Renewal of Service Providers registration is at the sole discretion of the Corporation.
4. To maintain the registration of a Service Provider, the Customer must submit such information and material as may be required by the Corporation from time to time, including but not limited to a copy of the agreement between the Customer and the Service Provider.
5. A Service Provider performing Program Service to one or more Customers must be distinctly proposed for registration with the Corporation on behalf of each Customer wanting to receive Program Service from that Service Provider.
6. A Service Provider performing more than one Program Service for a Customer must be distinctly proposed for registration with the Corporation for each Program Service provided from that Service Provider.
7. The Customer must receive the Corporation's written confirmation of the registration before:
   a. The Customer or any of such Customer's Sponsored Affiliates or any of their Service Providers or Merchants or Submerchants or, if applicable, Account Holders receive Program Service from the proposed Service Provider; or
   b. The proposed Service Provider commences performing such Program Service or represents itself to any person as authorized to provide such Program Service on behalf of the Customer or any of such Customer's Sponsored Affiliates.
8. The Customer must establish procedures for, and provide, oversight of any AML/Sanctions Service Provider. If any AML/Sanctions Service Provider interferes with a Customer's ability to comply with Rule 1.2, the Customer must notify the Corporation, take steps to remediate, and validate such remedial actions to the Corporation.

7.10.1 Site Data Protection (SDP) Program Noncompliance

Each Customer that has registered or proposed the registration of a TPP, SDWO, DASP, TSP, 3-DSSP, DSE, PF, TS, Installment Service Provider, or an AML/Sanctions Service Provider to provide Program Service for such Customer and/or any of such Customer's Sponsored Affiliates must promptly notify each of such Customer's Merchants, Submerchants, and any other entity that may be impacted by the Program Service if the registered or proposed Service Provider is not fully compliant with the applicable SDP Program requirements.

Notice must be made by the date on which the Program Service commences, or immediately if Program Service has commenced.

Such notification must include, with respect to the registered or proposed Service Provider:

1. The name and address of the Service Provider;
2. A description of the Program Service to be or being provided by the Service Provider;
3. A description of SDP Program requirements the Service Provider is not compliant with; and

4. A specific date by which the Service Provider will become fully compliant with applicable SDP Program requirements, or, in the alternative, the date by which the Service Provider will cease providing Program Service.

The application of such a Service Provider will not be approved until such time as the Service Provider becomes fully compliant with SDP Program requirements.

7.10.2 Registration Requirements for Type I TPPs

A TPP that the Corporation determines to be a Type I TPP, upon receiving notification of such determination, must apply to be registered by the Corporation as a Type I TPP, as follows.

Within 90 days of receiving notification of such Service Provider's designation by the Corporation as a Type I TPP, the TPP must submit TPP Registration Form 919 SSAE 18 or ISAE 3402 (or a Corporation approved equivalent standard) form and business continuity form using email to tpp_registration@mastercard.com.

Each Type I TPP must advise the Corporation promptly in writing when such Type I TPP commences to perform or ceases to perform any Program Service for any Customer, and on an ongoing basis, inform the Corporation of all ICA numbers pertaining to which such Type I TPP is performing any Program Service.

Registration as a Type I TPP is no longer available in the Europe Region. Any existing Type I TPP may remain a Type I TPP.

NOTE: A Rule on this subject appears in the "United States Region" chapter.

7.10.3 Registration Requirements for Type III TPPs

NOTE: A Rule on this subject appears in the "United States Region" chapter.

7.10.4 Registration Requirements for Installment Service Providers

Each Principal and Association, for itself and each of its Sponsored Affiliates, that issues or proposes to issue Cards for use in an Installment Card Program must register the Installment Service Provider it intends to use or uses in accordance with the following procedures:

1. Provide evidence satisfactory to the Corporation that the Installment Service Provider is in compliance with Mastercard Anti-Money Laundering and Sanctions Requirements.
2. Provide evidence satisfactory to the Corporation that the Installment Service Provider has the requisite authority to undertake the Activity.

7.10.5 Registration Requirements for Digital Activity Service Providers

The following requirements apply to registration of a Digital Activity Service Provider.

1. The Customer must receive the Corporation's written confirmation of the registration before:

a. The Principal, Association, a Sponsored Affiliate, or the Digital Activity Customer receive Program Service from the proposed DASP; or
b. The proposed DASP commences performing such Program Service or represents itself to any person as authorized to provide such Program Service on behalf of the Principal, Association, a Sponsored Affiliate, or the Digital Activity Customer.

7.10.6 Service Provider Registration Noncompliance

A Customer that fails to comply with these Service Provider registration requirements is subject to noncompliance assessments of up to USD 25,000 for each 30-day period of noncompliance.

7.11 Network Enablement Partners

The Rules in this Section are variances and additions to the Rules in Chapters 1 through 10 that apply to Network Enablement Partners.

7.11.1 Network Enablement Partner Eligibility

A Service Provider eligible to be a Network Enablement Partner:

- May apply to become a Network Enablement Partner; or
- May be designated by the Corporation to be a Network Enablement Partner, when deemed by the Corporation to be operationally significant to a Customer or Customers' performance in the Interchange System.

The decision to approve an application from or designate a Service Provider as a Network Enablement Partner is made at the sole discretion of the Corporation.

7.11.2 Network Enablement Partner Agreement Requirements

A Service Provider that applies to become a Network Enablement Partner or is designated by the Corporation to be a Network Enablement Partner must enter into a Network Enablement Partner Agreement prior to becoming a Network Enablement Partner.

A Service Provider designated by the Corporation to be a Network Enablement Partner must provide all information and materials required by the Corporation in connection with such designation by completing and submitting the NEP Application form to service_provider@mastercard.com, as applicable, and must enter into a Network Enablement Partner Agreement within thirty (30) days of the Corporation's notice to the Service Provider of such designation. During the thirty (30) day period, the Service Provider must work in good faith to execute the Network Enablement Partner Agreement with the Corporation. If after such thirty (30) day period, the Service Provider has not executed a Network Enablement Partner Agreement:

1. The Corporation will notify Customers using such Service Provider that such Customers must promptly terminate using such Service Provider for any Program Services on or before 180 days of such notification from the Corporation; and
2. No Customer will be able to register such Service Provider for any Program Services;

provided that such termination and inability to register may be remedied upon either (a) the Service Provider's execution of a Network Enablement Partner Agreement or (b) the Service Provider revising its business so as to no longer be designated by the Corporation to be operationally significant to a Customer or Customers' performance in the Interchange System.

A Service Provider that seeks to apply to become a Network Enablement Partner must

- complete and submit the NEP Application form to service_provider@mastercard.com; and
- within 30 days of the application submission date, provide all information and materials required by the Corporation in connection with such application to the My Company Manager application or via email to service_provider@mastercard.com, as applicable.

Each Network Enablement Partner must advise the Corporation promptly in writing when such Network Enablement Partner commences to perform or ceases to perform any Program Service for any Customer, and on an ongoing basis, inform the Corporation of all ICA numbers pertaining to any such Network Enablement Partner that is performing any Program Service.

7.11.3 Network Enablement Partner Services and Performance of Program Service

A Network Enablement Partner may only perform the Program Services such Network Enablement Partner is registered by the Customer to perform as a Service Provider.

A Network Enablement Partner must:

1. Be a Service Provider in good standing with the Corporation;
2. Satisfy all of the obligations and eligibility requirements for the underlying Service Provider Program for which such Network Enablement Partner is providing services;
3. Meet any and all requirements designated by Mastercard, including any capital requirements;
4. Comply with all Standards applicable to being a Network Enablement Partner and the Program Service provided (including, by way of example and not limitation, these Network Enablement Partner Rules, the Service Provider Rules, data use and protection, confidentiality and privacy Standards) for so long as such entity is a Network Enablement Partner and/or performs such Program Service. Network Enablement Partner obligations arise and continue regardless of the nature of the Program Service performed and whether the entity is performing Program Service pursuant to an agreement or other arrangement with the Customer, a Service Provider of the Customer, or any other entity;
5. Comply with section 13.1.2, "Service Provider Risk Management Program," of the *Security Rules and Procedures* manual, receiving at least a good rating or be in the process of mitigating any risk areas identified;
6. Pay any fees, including any registration and renewal fees, charged by the Corporation to a Network Enablement Partner. Renewal of Network Enablement Partner registration is at the sole discretion of the Corporation; and
7. Promptly provide to the Corporation any information requested by the Corporation pertaining to the Program Service or the performance thereof.

7.11.4 Applicability of Standards

7.11.4.1 General Applicability

The following Rules in Chapters 1 through 10 apply to Network Enablement Partners as if such Network Enablement Partner was a Customer:

- Rule 2.2.7 Information Security Program
- Rule 2.3 Indemnity and Limitation of Liability
- Rule 2.4 Choice of Laws
- Rule 2.5 Examination and Audit (for the avoidance of doubt, the Corporation's right to conduct any such examination or audit of the Network Enablement Partner includes any actual or suspected Account Data Compromise Event or ADC Event (as defined in the *Security Rules and Procedures* manual) and/or Personal Data breaches)
- Rule 3.7 Integrity of Brand and Network
- Rule 3.8 Fees, Assessments, and Other Payment Obligations
- Rule 3.8.1 Taxes and Other Charges
- Rule 3.15 Cooperation

7.11.4.2 Mastercard Anti-Money Laundering and Sanctions Requirements

Rule 1.2 applies to Network Enablement Partners as if such Network Enablement Partner was a Customer, and Rule 1.2.1, and Rule 1.2.2, are amended and restated to apply to Network Enablement Partners as follows:

1.2.1 Anti-Money Laundering Requirements

Each Network Enablement Partner must have AML controls in place for all Activity to safeguard the Corporation and the Interchange System from and against the use of the Interchange System for money laundering and/or terrorist financing. These AML controls, must be commensurate with the Network Enablement Partner's respective AML risk profile, be fully implemented in accordance with this Rule and local regulatory requirements, and include at a minimum, the following:

1. A process to ensure thorough client identification and due diligence; and
2. Sufficient controls, resources, and monitoring systems for the prompt detection and reporting of suspicious activity.

To the extent applicable, each Network Enablement Partner must comply with the requirements set forth in Rule 1.2.1.1 as if such Network Enablement Partner was a Customer.

1.2.2 Sanctions Requirements

Each Network Enablement Partner, regardless of where situated, must ensure that Activity is in compliance with the sanctions laws and regulations enacted by United States sanctions authorities (including, the United States Office of Foreign Assets Control ["OFAC"] and the United States Department of State), as well as all applicable local sanctions regulations where the Activity is taking place.

A Network Enablement Partner is prohibited from engaging in Activity with any person, including any legal entity or government, or in any geography in contravention of any regulation

or other requirement promulgated by the United States sanctions authorities, as well as any applicable local sanctions authority.

Sanctions List Screening

A Network Enablement Partner must screen the Customer engaging with the Network Enablement Partner and if engaged in Program Services that provide services to Cardholders, Merchants, Originating Account Holders, Receiving Account Holders or other representatives and agents covered by the screening requirements in Rule 1.2.2, must screen such persons, in each case at the time of onboarding and on an ongoing basis, against applicable sanctions lists, including, but not limited to, OFAC sanctions lists (such as, the Specially Designated Nationals and Blocked Persons List [the "SDN List"]).

Prohibited Activity

1. No Activity may be conducted in a geography (country or region) that is the subject of applicable sanctions, including those identified by OFAC.
2. No Activity may be conducted with a person, entity, or government on the OFAC sanctions lists (such as, the SDN List) and other locally applicable sanctions lists.

A Network Enablement Partner must immediately cease any Activity with a person, entity, or government identified as listed on any of the OFAC sanctions lists or locally applicable sanctions lists.

NOTE: Activity with an entity listed on OFAC's Sectoral Sanctions Identifications List ("SSI List") may only be conducted in compliance with the limitations or conditions established by OFAC for that program.

7.11.4.3 Variances

A Network Enablement Partner may request a variance pursuant to Rule 2.1.1.

7.11.4.4 Failure to Comply with a Standard

Rules 2.1.2 through 2.1.7 apply to each Network Enablement Partner as if such Network Enablement Partner was a Customer; provided that:

1. Each Network Enablement Partner acknowledges and agrees that such Network Enablement Partner and Customer(s) who registered the Network Enablement Partner for Program Services are jointly and severally liable for any failure by the Network Enablement Partner to comply with the Standards.
2. While each Customer is responsible for any failure to comply with any Standard (including by a Service Provider of a Customer, whether or not such Service Provider is also a Network Enablement Partner) and is subject to noncompliance assessments as set forth in the Standards, if failure to comply with a Standard by more than one Customer is related to a Network Enablement Partner's failure to comply with a Standard:

- The Corporation may apply assessments to the Network Enablement Partner and the Customer(s) who registered the Network Enablement Partner for Program Services in accordance with Rule 2.1.4.
- In lieu of, or in addition to, the imposition of a noncompliance assessment, the Corporation, in its sole discretion, may require the Network Enablement Partner and the applicable Customer or Customers to take such action and the Corporation itself may take such action as the Corporation deems necessary or appropriate to ensure compliance with the Standards and safeguard the integrity of the Interchange System. In the exercise of such discretion, the Corporation may consider the nature, willfulness, number and frequency of occurrences and possible consequences resulting from a failure to comply with any Standard. The Corporation may provide notice and limited time to cure such noncompliance before imposing a noncompliance assessment. The Corporation reserves the right to limit, suspend or terminate a Network Enablement Partner's Network Enablement Partner Agreement and/or ability to provide Program Services to any Customer or to amend the rights, obligations, or both of the Network Enablement Partner, if that Network Enablement Partner does not comply with any Standards or with any decision of the Corporation with regard to the interpretation and enforcement of any Standards.

3. Rule 2.1.5 is amended and restated as follows: A senior executive officer of each Network Enablement Partner must, if requested by the Corporation, promptly certify in writing to the Corporation the status of compliance or noncompliance with any Standard by the Network Enablement Partner or by any Customer for which it performs a Program Service.

7.11.4.5 Testing of Assets

A Network Enablement Partner may apply to the Corporation to participate in the testing of assets of the Corporation (for example, an ICA or a BIN). The Corporation may permit such testing at its discretion.

Use of an ICA and/or BIN may not be sublicensed or re-assigned or otherwise transferred without the prior express written consent of the Corporation.

The Corporation may:

- Review a Network Enablement Partner's ICA and/or BIN usage for compliance with the Standards; and
- Retract the permission of any ICA and/or BIN that has been granted for technical purposes to a Network Enablement Partner.

7.11.5 Network Enablement Partner Requirements

7.11.5.1 Notification to the Corporation of Change of Name or Transfer of Ownership or Control

Each Network Enablement Partner must advise the Corporation promptly in writing when it:

1. Undergoes a change of name or transfer of Ownership or Control;
2. Fails or refuses to make payments owed in the ordinary course of business;

3. Makes an assignment for the benefit of creditors; or
4. Seeks bankruptcy protection or similar protection.

7.12 Prohibition from Acting as a Service Provider

The Corporation reserves the right to prohibit a Service Provider, a Service Provider's owners, and/or a Service Provider's employees from performing Program Service; acting as a DSE, TS, or 3-DSSP; being a Network Enablement Partner; or all.

7.13 Termination of a Service Provider, Program Service Agreement, Network Enablement Partner Agreement or De-registration

If any of the following occurs, the Customer must notify the Corporation of the date and reasons for such action:

- The Customer terminates a Service Provider,
- The Customer ceases to accept Submerchant Transactions from a Payment Facilitator,
- The Customer ceases to accept Transactions from a DCC Service Provider,
- The agent for a Customer or a Merchant terminates a Terminal Servicer or 3-D Secure Service Provider, or
- The Customer's Service Provider otherwise ceases to perform the Program Service for which such Service Provider was registered.

If a Type I TPP or a Network Enablement Partner terminates or ceases to perform the applicable Service Program, the Type I TPP or a Network Enablement Partner must notify the Corporation of the date and reasons for such action.

The Customer, Type I TPP or Network Enablement Partner, as the case may be, must use the My Company Manager application on Mastercard Connect™ to notify the Corporation of any such change in status and provide all information and material required by the Corporation in connection with such change in status to the My Company Manager application or service_provider@mastercard.com, within one week of the decision.

In the Corporation's sole discretion, the Corporation may, at any time, (1) require a Customer to terminate a Service Provider, (2) require an Acquirer to cease to accept Submerchant Transactions from a Payment Facilitator or Transactions from a DCC Service Provider, (3) terminate the participation of a Type I TPP or (4) terminate a Network Enablement Partner Agreement, including if a Service Provider:

a. Fails to comply with any applicable Standards, including, if applicable, the Corporation's Anti-Money Laundering and Sanctions Requirements;

b. (i) Directly or indirectly engages in or facilitates any action or activity that is illegal, or that, in the good faith opinion of the Corporation, and whether or not addressed elsewhere in the Standards, has damaged or threatens to damage the goodwill or reputation of the Corporation or of any of its Marks; or (ii) makes or continues an association with a person or entity and such

association, in the good faith opinion of the Corporation, has damaged or threatens to damage the goodwill or reputation of the Corporation or of any of its Marks; or

c. (i) Provides to the Corporation inaccurate material information or fails to disclose responsive material information in or in connection with its performing a Program Service; or (ii) at any other time, in connection with its performing a Program Service fails to timely provide to the Corporation information requested by the Corporation and that the Customer is required to provide pursuant to the terms of Standards.

(1) On the effective date of the termination or expiration of the Program Service agreement, or a Network Enablement Partner Agreement, (2) upon notice by the Corporation, (3) upon expiration or de-registration of an entity as a Service Provider or Network Enablement Partner, or (4) upon such other date as provided by the Corporation for purposes of the orderly wind down or transfer of such Program Service

A. the entity must immediately cease all use of the Corporation's systems and Marks and cease performing the Program Service and cease all participation in any activities on the Interchange System; and

B. the entity is not entitled to any refund of dues, fees, assessments, or other payments and remains liable for, and must promptly pay to this Corporation (i) any and all applicable dues, fees, assessments, or other charges as provided in the Standards and (ii) all other charges, debts, liabilities, and other amounts arising or owed in connection with the entity's Program Service, whether arising, due, accrued, or owing before or after termination, expiration or de-registration.

7.14 Confidential Information of Service Providers

With regard to any Service Provider, and regardless of (i) how the Service Provider is or may be categorized, (ii) the nature of Program Services the Service Provider may perform, and (iii) whether the Service Provider is registered as a Service Provider by the Corporation, the following information is not confidential information:

1. The name, address and other contact information of the Service Provider;
2. The identity of any Customer the Corporation believes may be receiving Program Services by the Service Provider;
3. The nature of Program Services the Corporation believes the Service Provider may be performing for any Customer; and
4. Any information the Corporation deems necessary or appropriate to disclose in order to safeguard the financial, reputational or other interests of the Corporation, Customers, or both.

7.15 Audits

In addition to the audit rights of the Corporation with respect to Network Enablement Partners set forth in Rule 7.11.4.1, the Corporation or the Corporation's designee may conduct one or

more regular or periodic financial and procedural audits of the Customer, the Customer's Service Providers, or both, at any time and from time to time for the purpose of determining compliance with the Standards, including these Service Provider Rules. The Customer bears all costs of any such audit or audits. The Customer and the Customer's Service Providers each must fully co-operate with and promptly supply the Corporation with all information and material upon request.

7.16 No Endorsement by the Corporation

In no event does compliance with these Service Provider Rules or enforcement or any lack of or delay in enforcement thereof or the registration of a Service Provider or execution of a Network Enablement Partner Agreement imply, suggest, or otherwise mean that the Corporation endorses any Service Provider, any Network Enablement Partner or the nature or quality of Program Service or other performance or that the Corporation approves of, is a party to, or a participant in, any act or omission by a Service Provider, a Network Enablement Partner or other entity acting for or on behalf of a Customer.

Chapter 8 Settlement and Related Obligations

This chapter contains Rules relating to interchange and service fees, settlement, and other financial obligations.

8.1 Definitions

As used in the Rules set forth in this section, the following terms have the meanings described:

1. "Interchange fee" means an amount paid by the Acquirer to the Issuer with respect to the interchange of a Transaction conducted by a Merchant or a Merchandise Transaction conducted at an ATM Terminal. All references to interchange fees in this section mean both the levels of the fees and all qualifying criteria and conditions for their applicability.
2. "Intracountry issuing Volume" means the issuing Volume resulting from Intracountry Transactions.
3. "Intracountry acquiring Volume" means the acquiring Volume resulting from Intracountry Transactions.
4. "Service fee" means an amount paid by the Issuer to the Acquirer with respect to the interchange of a Manual Cash Disbursement Transaction or ATM Transaction. All references to service fees in this section mean both the levels of the fees and all qualifying criteria and conditions for their applicability.

NOTE: Modifications to this Rule appear in the "Europe Region" chapter.

8.2 Net Settlement

A Customer that uses the Interchange System for the authorization and clearing of Transactions is required to net settle in accordance with the Corporation's settlement Standards.

However, an Acquirer and an Issuer may, with respect to a particular Transaction, agree to settle directly between themselves pursuant to a bilateral agreement.

Standards describing net settlement and bilateral agreement rights and obligations are set forth in the *Settlement Manual*. For information about Single Message System settlement options, refer to *Single Message System Settlement and Reports*.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

8.2.1 Currency Conversion

The Corporation converts Transactions processed through use of the Interchange System into the applicable settlement currency.

The Acquirer must submit each Transaction in the currency in which it occurred.

If two Customers elect not to settle a Transaction by using the Interchange System and instead elect to settle directly between themselves in accordance with a bilateral agreement, any Transaction currency that the Corporation supports is acceptable for settlement.

NOTE: Modifications to this Rule appear in the "Europe Region" and "Latin America and the Caribbean Region" chapters.

8.2.2 Settlement Messages and Instructions

NOTE: Rules on this subject appear in the "Europe Region" chapter.

8.2.3 Reconciliation

It is the responsibility of each Customer to reconcile the totals and Transactions provided by the Interchange System to its own internal records on a daily basis.

For more information on reconciliation, refer to *Single Message System Programs and Services* and the *GCMS Reference Manual*.

8.3 Interchange and Service Fees

A Transaction settled between Customers gives rise to the payment of the appropriate interchange fee or service fee, as applicable.

The Corporation has the right to establish default interchange fees and default service fees (hereafter referred to as "interchange fees," "service fees," or collectively, "fees"), it being understood that all such fees set by the Corporation apply only if there is no applicable bilateral interchange fee or service fee agreement between two Customers in place. The Corporation establishes all fees for Interregional Transactions and Intraregional Transactions, and may establish fees for Intracountry Transactions.

The Corporation will inform Customers, as applicable, of all fees it establishes and may periodically publish fee tables. Unless an applicable bilateral interchange fee or service fee agreement between two Customers is in place, any intraregional or interregional fees established by the Corporation are binding on all Customers.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region" and "Europe Region" chapters.

8.3.1 Cost Studies

The Corporation or its agent may conduct one or more cost studies on a country-specific or regional or other basis for the purpose of establishing interchange and service fees.

In order to ensure a sufficient quantity and level of data quality and representativeness as the Corporation deems necessary, the Corporation may designate any number of Customers to participate in cost studies. Each Customer so designated is required to participate and must provide and be able to certify that it has provided the Corporation or its agent with complete and accurate information in the form and manner and for such period of time and by a date as requested.

8.3.1.1 Allocation of Expenses

The Corporation may allocate expenses related to any cost study among Customers conducting Activity in the country or region or other area that is the subject of the cost study.

The expenses may be allocated as the Corporation deems appropriate and the decision of the Corporation is binding on all Customers in that country or region or other area.

8.3.1.2 Compliance with a Cost Study

A Customer designated to participate in a cost study that fails to fully and timely participate is subject to assessments and other disciplinary action at the sole discretion of the Corporation.

8.4 Establishment of Intracountry Interchange and Service Fees

This rule is applicable only to Intracountry Transactions.

Unless prohibited by applicable law, default intracountry interchange and service fees are established by the Corporation, or by application of intraregional interchange or interregional interchange and service fees to Intracountry Transactions as set forth in Rule 8.4.1. Such fees may also be established by bilateral agreement between two Customers as set forth in Rule 8.4.2.

For any Transaction that is subject to a bilateral agreement between two Customers, the interchange and service fees set forth in the bilateral agreement prevail.

For any Transaction that is not subject to a bilateral agreement between two Customers, the default intracountry fees established by the Corporation apply, or if none, the intraregional fees apply, or if none, the interregional fees apply. The Corporation reserves the right to determine if multiple bilateral agreements are deemed to be a multilateral agreement.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region" and "Latin America and the Caribbean Region" chapters.

8.4.1 Intraregional Fees

In the event that no bilaterally agreed interchange fee or service fee applies and no default interchange fee or service fee has been established pursuant to these Rules, the applicable intraregional fee or if none, the interregional fee, applies to Intracountry Transactions.

NOTE: A modification to this Rule appears in the "Asia/Pacific Region" chapter.

8.4.2 Bilateral Agreement

Any two Customers may establish, by bilateral agreement, the interchange and service fees applicable to Transactions between them.

All such fees must be submitted promptly to the Corporation. When applicable to Transactions processed through the Interchange System, they must be submitted to the Corporation sufficiently in advance of the effective date to allow the Corporation to incorporate the fees into future Interchange System releases as necessary.

NOTE: Modifications to this Rule appear in the "Asia/Pacific Region" and "Europe Region" chapters.

8.5 Failure of a Principal or Association to Discharge a Settlement Obligation

Subject to the limitation set forth in this Rule, if a Principal or Association fails to discharge a Settlement Obligation arising from or in connection with any Processed Transaction, the Corporation will satisfy such Settlement Obligation to the extent such Settlement Obligation is not otherwise satisfied.

To the extent the Corporation satisfies a Customer's Settlement Obligation, such satisfaction constitutes an automatic transfer, sale, and absolute assignment to the Corporation, and not an assignment for security purposes, of all right, title, and interest in the receivable. Such satisfaction of the Customer's Settlement Obligation also entitles the Corporation to all records and documents related to the receivable, including the name and address of each Cardholder or other person obligated to satisfy any part of the receivable. The Customer must promptly deliver all such records and documents to the Corporation or to the Corporation's designee. Any proceeds received by or on behalf of the Customer from any receivable must be held in trust by the Customer and paid to the Corporation as soon as practicable.

The Corporation may take any action the Corporation deems necessary or appropriate to protect its interest in the receivable and to protect the integrity of the affairs of the Corporation, such as, by way of example and not limitation, by:

1. Refusing or rejecting Transaction authorization requests relating to use of the Customer's Cards or refusing or rejecting Payment Transfer Activity (PTA) Transaction initiation requests.
2. Without prior notice to the Customer, holding any monies due, directly or indirectly and for any purpose, to the Customer from the Corporation and any Settlement Obligations due to the Customer and apply those monies to the amounts the Customer owes to the Corporation and to other Customers arising from Activity.
3. Listing some or all of a Customer's Account numbers on the Electronic Warning Bulletin file, the international Warning Notices, or both, or in other or similar publications.
4. Effecting chargebacks on behalf of the Customer.
5. Overseeing the disposition of unused Card stock and any other media bearing security-sensitive information, including Account information.

The Corporation assumes no liability, responsibility, or obligation to satisfy, in full or in part:

A. A Settlement Obligation arising from or in connection with a Transaction that was not a Processed Transaction.

B. A Settlement Obligation arising from or in connection with a Transaction in which the Principal or Association, considered together with one or more of its Affiliates, acts as both the Issuer and the Acquirer

C. A Settlement Obligation arising from or in connection with a Transaction in which the Issuer and Acquirer are related parties or are under common Control by one or more parents, holding companies, or other entities.

D. A Settlement Obligation arising from or in connection with any of the Principal's or Association's Sponsored Affiliates.

E. A Settlement Obligation arising from or in connection with an Intracountry Transaction that was not settled, in whole or in part, where the non-settlement was expressly directed, mandated, or otherwise compelled by a government or governmental regulatory agency, regardless of whether such direction or mandate was publicly announced. For clarity, this provision shall not apply where the nonsettlement occurred at the direction of a government or government-designated receiver or trustee made in the ordinary course of a receivership/insolvency proceeding.

NOTE: A modification to this Rule appears in the "Europe Region" and "Latin America and the Caribbean Region" chapters.

Payment Transfer Activity Variation

The Rule on this subject, as it applies to Payment Transfer Activity is revised and restated as follows.

Only Processed PTA Transactions conducted pursuant to a PTA Settlement Guarantee Covered Program are covered by this Rule 8.5.

Subject to the limitation set forth in this Rule, if a Principal or Association Originating Institution fails to discharge a PTA Settlement Obligation arising from or in connection with any first presentment Processed PTA Transaction for a PTA Settlement Guarantee Covered Program, the Corporation will satisfy such PTA Settlement Obligation to the extent such PTA Settlement Obligation is not otherwise satisfied.

To the extent the Corporation satisfies a Customer's PTA Settlement Obligation, such satisfaction constitutes an automatic transfer, sale, and absolute assignment to the Corporation, and not an assignment for security purposes, of all right, title, and interest in the receivable. Such satisfaction of the Customer's PTA Settlement Obligation also entitles the Corporation to all records and documents related to the receivable, including the name and address of each Account Holder or other person obligated to satisfy any part of the receivable. The Customer must promptly deliver all such records and documents to the Corporation or to the Corporation's designee. Any proceeds received by or on behalf of the Customer from any receivable must be held in trust by the Customer and paid to the Corporation as soon as practicable.

The Corporation may take any action the Corporation deems necessary or appropriate to protect its interest in the receivable and to protect the integrity of the affairs of the Corporation, such as, by way of example and not limitation, by:

1. Refusing or rejecting PTA Transaction initiation requests or refusing or rejecting any Transaction authorization requests relating to use of the Customer's Cards.
2. Without prior notice to the Customer, holding any monies due, directly or indirectly and for any purpose, to the Customer from the Corporation and any PTA Settlement Obligations due to the Customer and apply those monies to the amounts the Customer owes to the Corporation and to other PTA Customers.

3. Listing some or all of the PTA Account Numbers or Account numbers held by or on behalf of such Customer on the Electronic Warning Bulletin file, the international Warning Notices, or both, or in other or similar publications.
4. Effecting chargebacks on behalf of an affected PTA Customer, if available.
5. Overseeing the disposition of any media bearing security sensitive information, including PTA Account information.

The Corporation assumes no liability, responsibility, or obligation to satisfy, in full or in part:

A. A PTA Settlement Obligation arising from or in connection with a PTA Transaction that was not a Processed PTA Transaction.

B. A PTA Settlement Obligation arising from or in connection with a PTA Transaction in which the PTA Customer, considered together with one or more of its Affiliates, acts as both the Originating Institution and the Receiving Customer.

C. A PTA Settlement Obligation arising from or in connection with a PTA Transaction in which the Originating Institution and the Receiving Customer are related parties or are under common Control by one or more parents, holding companies, or other entities.

D. A PTA Settlement Obligation arising from or in connection with any of the PTA Customer's Principal's or Association's Sponsored Affiliates.

E. A PTA Settlement Obligation arising from or in connection with a PTA Transaction that was not settled, in whole or in part, where the non-settlement was expressly directed, mandated, or otherwise compelled by a government or governmental regulatory agency, regardless of whether such direction or mandate was publicly announced. For clarity, this provision shall not apply where the non-settlement occurred at the direction of a government or government-designated receiver or trustee made in the ordinary course of a receivership/insolvency proceeding.

NOTE: A modification to this Payment Transfer Activity variation appears in the "Europe Region" and "Latin America and the Caribbean Region" chapters.

8.6 Settlement Liability for Debit Licensees

NOTE: A Rule on this subject appears in the "United States Region" chapter.

8.7 Settlement Liability for Type I TPPs that Sponsor Affiliates

NOTE: A Rule on this subject appears in the "United States Region" chapter.

8.8 System Liquidity

If the Corporation requires funds to maintain system liquidity and to meet the obligations that a Customer or Customers have failed to discharge (for purposes of this section, "Non-discharged Customer Obligations"), the Corporation may collect funds directly from the settlement accounts of Customers upon reasonable notice to the Customers.

In such event, the funds will be collected by the Corporation by:

1. Decreasing the gross daily settlement amounts of outgoing volumes of Customers by up to five percent (5 percent) of the amount settled on one or more days; and
2. Increasing the gross daily settlement amounts of incoming volumes of Customers by up to five percent (5 percent) of the amount settled on one or more days.

This collection may continue as long as deemed necessary or appropriate to satisfy Non-discharged Customer Obligations and to ensure system liquidity or until the Corporation deems such collection no longer necessary or appropriate.

Collected funds are treated as advance payments on the sums that may be required from the Customers in the allocation among Customers of loss related to Non-discharged Customer Obligations. If the funds collected from a Customer exceed the amount ultimately allocated to it in connection with Non-discharged Customer Obligations, the excess amount will be returned to the Customer with interest. If the funds collected from a Customer do not exceed the amount allocated to it, the Customer will pay any shortage to the Corporation with interest. Any interest payment by or to the Corporation will be based on the average effective Federal Reserve Fund's Earning Credit Rate (or if such rate is not published, a rate that the Corporation designates) during the time between the incidence of the Customer funding and the final allocation.

NOTE: A modification to this Rule appears in the "Europe Region" chapter.

8.9 Liability for Owned or Controlled Entities

Each Customer (referred to for purposes of this Rule as a "Responsible Customer") shall irrevocably and unconditionally guarantee, as a primary obligor and not merely as a surety, to the Corporation and all other Customers, the prompt payment and performance of the obligations (the "Guaranteed Obligations") of each of the Responsible Customer's affiliated entities arising under the Standards and from each such affiliated entity's Mastercard, Maestro, and Cirrus Activities and use of any of the Marks.

For purposes of this Rule, a Responsible Customer's affiliated entity is defined as follows:

1. A Customer that is Owned or Controlled by the Responsible Customer or is owned or controlled by the Responsible Customer and another Customer or Customers; or
2. A Customer that, with the Responsible Customer, is under common Ownership by, or Control of, another entity; or

3. A Customer that Owns or Controls the Responsible Customer or shares Ownership or Control of the Responsible Customer with another Customer or Customers.

The obligations of each Responsible Customer under this Rule shall be continuing, absolute, and unconditional and shall not be discharged or impaired or otherwise affected by any act or omission (including any renewal, extension, amendment, waiver or unenforceability of any of the Guaranteed Obligations) that may vary the risk of such Responsible Customer or otherwise operate as a discharge of the obligations of such Responsible Customer as a matter of law or equity, and all defenses of the Responsible Customer with respect thereto are waived to the fullest extent permitted by applicable law.

The Responsible Customer's liability to the Corporation and all other Customers is a primary obligation, while the Corporation's liability, if any, to another Customer is secondary, in that it only arises if a Responsible Customer is unable to pay its Guaranteed Obligations in full. Any assessments imposed on a Customer for liability under this Rule may be collected by the Corporation, at its option, from the Customer's settlement account or by any other means available. A Responsible Customer may not be exempted from this Rule except upon written notice by the General Counsel of the Corporation.

8.10 Risk of Loss

Each Customer bears all risk of loss and the Corporation bears no risk of loss with respect to all amounts owed by the Customer related to the settlement except to the extent any such amount is received by the Corporation, free and clear.

Each Customer remains fully responsible for fulfillment of, and must take all actions necessary to fulfill, all of its obligations under the Standards, regardless of whether the Customer designates a Service Provider or other third party to perform all or any part of such obligations on the Customer's behalf. The fact that a Customer has paid any portion of any amount owed to any such third party designee does not discharge any of the Customer's obligations to the Corporation.

The Corporation may draw on the Customer's funds to fulfill any one or more of the Customer's obligations under the Standards, regardless of whether those funds are held or controlled by the Customer or by any third party designee, to the same extent that the Corporation is entitled to draw on funds from any settlement account or funds of the Customer in accordance with the Standards, and regardless of whether those funds are commingled with any other funds. If the Corporation draws on the Customer's funds in accordance with the Standards, the Corporation is not required to reimburse the Customer or any third party (whether a third party designee of the Customer or another Customer) for funds drawn which are owned by any of them or otherwise subject to any of their rights. The Customer and any third party (whether a third party designee of the Customer or another Customer) bear all risk and liability related to the funds drawn and must jointly and severally indemnify and hold the Corporation harmless from all liability and claims arising from any such draw of funds.

Each Customer bears all risk of loss, and the Corporation bears no risk of loss with respect to all amounts owed by the Corporation to the Customer under the Standards once the Corporation

has discharged the Corporation's obligations set forth in the *Settlement Manual*, regardless of whether the payment is received by the Customer or a third party designee of the Customer.

Each Customer must notify the Corporation promptly in writing if any third party designee commingles funds received for or from the Customer in connection with the Customer's Transactions with any other funds. Each Customer must notify the Corporation promptly in writing of the details of any failure of the Customer or any third party designee of the Customer to meet any of their obligations with respect to payment of funds owed under the Standards.

If a Customer's third party designee advances funds on behalf of the Customer to pay the Corporation or any other party entitled to receive those funds in accordance with the Standards, then such payment is deemed to be a payment by the Customer, and the Customer, and the third party designee of the Customer, jointly and severally bear all risks of loss and must jointly and severally indemnify and hold the Corporation harmless from any and all liability and claims arising from any such payment.

In addition to the other Customer obligations set forth in this Rule 8.10, a Customer must:

1. Obtain the prior written agreement of any third party designee of the Customer that may be given access to any funds owed by or to the Customer pursuant to the Standards; and
2. Be responsible for any such third party designee's compliance with all applicable Standards, including those set forth in this Rule 8.10.

NOTE: Modifications to this Rule appear in the "United States Region" chapter.

8.11 Loss Allocation Among Customers

Any loss that the Corporation incurs, or for which the Corporation may otherwise be responsible due to the failure of a Mastercard Customer, whether or not intentional, to perform any of its Participation obligations, may be allocated among the Mastercard Customers by the Corporation in such manner and at such times as the Corporation determines to be appropriate.

NOTE: Modifications to this Rule appear in the "Latin America and the Caribbean Region" chapter. An addition to this Rule appears in the "Europe Region" chapter.

8.12 PTA Transaction Settlement

Each Originating Institution is required to settle any PTA Transaction and each Receiving Customer is required to settle any reversal, return, or chargeback of any PTA Transactions, in the manner (including within the relevant time period) required by applicable law or regulation, the Standards, and, if applicable, the Non Mastercard Systems and Network Standards.

Chapter 9 Digital Activity

This chapter contains Rules pertaining to Digital Activity and Digital Activity Customers.

Digital Activity Rules

The Standards for Digital Activity consist of these Digital Activity Rules; the technical specifications set forth in the *Authorization Manual* and *Single Message System Programs and Services*; and any other Rule that references Digital Activity, Digital Activity Customers, or the Mastercard Digital Enablement Service as amended from time to time.

Applicability of Rules

The Rules in this Digital Activity chapter are variances and additions to the Rules in Chapters 1 through 8 that apply solely to Digital Activity.

The Rules in Chapters 1 through 8 continue to apply to the Activity of a Customer. The following Rules pertain only to the conduct of Activity and **do not** apply to Digital Activity or to Digital Activity Customers:

- Rule 1.5 Interim Participation
- The subsections of Rule 1.7 Area of Use of the License
- Rule 1.9.1 Changing Customer Status
- Rule 1.9.3 Right to Sponsor Affiliates
- Rule 1.9.4 Change in Sponsorship of an Affiliate
- Rule 1.10 Participation in Competing Networks and its subsections
- Rule 1.11 Portfolio Sale, Transfer, or Withdrawal
- Rule 2.2.2 Obligations of a Sponsor
- Rule 2.2.3 Affiliates
- Rule 2.2.5 Mastercard Acquirers
- Rule 3.1 Obligation to Issue Mastercard Cards
- Rule 3.2 Responsibility For Transactions
- Rule 3.3 Transaction Requirements
- Rule 3.4 Authorization Service
- Rule 3.5 Non-Discrimination—POS Transactions
- Rule 3.6 Non-Discrimination—ATM and Bank Branch Terminal Transactions
- Rule 3.8.2 Maestro and Cirrus Card Fees and Reporting Procedures
- Rule 3.16 Issuer Reporting Requirement—EEA, Serbia, Gibraltar and United Kingdom
- Rule 3.17 BINs
- Rule 4.8 Use of Marks on Maestro and Cirrus Cards
- Rule 4.9 Use of Marks on Mastercard Cards
- Rule 4.10 Use of a Card Design in Merchant Advertising and Signage
- Rule 4.12 Use of the Mastercard Card Design in Cardholder Statement Enclosures
- Chapter 5 in its entirety
- Chapter 6 in its entirety
- Rule 7.2.7 Service Provider Identification on a Card

- Rule 7.2.9 Notification of Settlement Failure Obligation
- Rule 7.3 Access to Merchant Account
- Rule 7.6 Acquiring Programs and its subsections
- Rule 7.7 Issuing Programs and its subsections
- Rule 7.8 Payment Facilitator Obligations and its subsections
- Rule 7.9 Type I TPP Obligations
- Rule 7.10.2 Registration Requirements for Type I TPPs
- Rule 7.10.3 Registration Requirements for Type III TPPs
- Chapter 8 Settlement and Related Obligations in its entirety

1.1 Eligibility to be a Customer

The Rule on this subject, as it pertains to Digital Activity Customers, is replaced with the following.

An entity eligible to be a Digital Activity Customer may apply to become a Digital Activity Customer. No entity may participate in Digital Activity as a Digital Activity Customer until that entity is approved to be a Digital Activity Customer, has executed the applicable Digital Activity Agreement for the proposed Digital Activity in a form acceptable to the Corporation, and has paid all associated fees and other costs.

1.1.3 Digital Activity Customer

An entity that satisfies such eligibility criteria as the Corporation may adopt from time to time, consistent with the promotion of safe and sound business practices, may apply to be a Digital Activity Customer.

The decision to approve an applicant as a Digital Activity Customer is at the discretion of the Corporation.

The eligibility criteria for a Digital Activity Customer are:

1. Compliance with the *Payment Card Industry Data Security Standard (PCI DSS)*;
2. Compliance with all applicable laws and regulations for each jurisdiction in which the Digital Activity is proposed to be conducted, including but not limited to the existence of client data privacy policies and procedures and all necessary licenses and other permissions as may be required;
3. Compliance with all applicable Digital Activity Rules and related program documentation; and
4. The successful completion of such certification and testing procedures as the Corporation may require.

1.8 The Digital Activity Agreement

Each Digital Activity Customer must enter into a Digital Activity Agreement with the Corporation.

In the event of an inconsistency between a Rule or other Standard and a provision in a Digital Activity Agreement, the Rule or other Standard shall be afforded precedence and the Digital Activity Agreement is deemed to be amended so as to be consistent with the Rule or other Standard. Each Digital Activity Customer must assist the Corporation in recording any Digital Activity Agreement granted to the Customer if required in the country or countries in which the Digital Activity Customer is located or otherwise upon request of the Corporation.

Each Digital Activity Agreement shall include a limited License granting the Customer the right to use the Marks solely in connection with the conduct of the approved Digital Activity, in accordance with the Standards, and with no specified Area of Use.

1.9 Participation in Activity(ies) and Digital Activity

The Rule on this subject, as it applies to Digital Activity, is modified to add the following.

Each Digital Activity Customer and each other Customer approved by the Corporation to conduct Digital Activity may participate only in such Digital Activity as is set forth in its Digital Activity Agreement or Agreements with the Corporation or as otherwise documented in writing by the Corporation.

1.9.6 The Sponsored Digital Activity Entity

To propose the sponsorship of a Sponsored Digital Activity Entity, a Digital Activity Sponsoring Customer must be in good standing with the Corporation.

A Digital Activity Sponsoring Customer must at all times:

- Ensure that each Sponsored Digital Activity Entity complies on an ongoing basis with all applicable Standards;
- Be entirely responsible for and must manage, monitor, direct and control all aspects of the Digital Activity performed by a Sponsored Digital Activity Entity; and
- Not transfer or assign any part of such responsibilities or in any other way limit its responsibility with regard to a Sponsored Digital Activity Entity.

A Sponsored Digital Activity Entity:

- Must only conduct the Digital Activity for which the Digital Activity Sponsoring Customer is approved;
- Is a Customer for the limited purpose of conducting the Digital Activity of the Digital Activity Sponsoring Customer; and
- Is subject to Rule 1.12, "Change of Control of Customer or Portfolio."

3.12 Confidential Information of Mastercard

The Rule on this subject, as it applies to Digital Activity, is modified to add the following.

For purposes of this Rule, "the Corporation's Systems" means any of the Corporation's equipment and software and "the Corporation's Confidential Information" means any of the Corporation's information identified or reasonably understood to be confidential or proprietary.

Each Digital Activity Customer and each other Customer engaged in Digital Activity must:

1. Use any of the Corporation's Systems and any of the Corporation's Confidential Information to which it has access in connection with its Digital Activity Agreements solely to conduct the Digital Activities specified therein;
2. Treat the Corporation's Systems and Confidential Information at least as carefully and confidentially as the Customer treats its own systems and proprietary information;
3. Acknowledge that access to the Corporation's Systems and Confidential Information does not provide the Customer with any right to use them further;
4. Limit access to the Corporation's Systems and Confidential Information to those employees with a need to have access in order to enable the Customer to perform its Digital Activity and to implement and to maintain reasonable and appropriate safeguards to prevent unauthorized access to the Corporation's Systems or disclosure of the Corporation's Confidential Information, including those set forth in section 10.4 of the *Security Rules and Procedures* manual;
5. Immediately cease any use of the Corporation's Systems and Confidential Information upon request of the Corporation or upon the termination of its Digital Activity Agreements, and to immediately deliver all of the Corporation's Systems and Confidential Information to the Corporation; and
6. Immediately advise the Corporation if any unauthorized person seeks to gain or gains access to the Corporation's Systems or Confidential Information, whether by legal proceedings or otherwise.

9.1 Digital Activity and Conduct of a Staged Digital Wallet Operator

Rules on this subject appear below.

9.1.1 General Obligations

A Digital Activity Customer and Staged DWO must:

- Avoid undue risk to the Corporation and its Customers;
- Be operated in a manner that does not reflect poorly on the Corporation or any Mark;
- Use any Mastercard or Maestro Mark, Issuer's logo, or Digital Card Image in accordance with the Standards and/or permission granted by the respective owner;

- Not disparage the Corporation or any of the Corporation's products, programs, services, networks, or systems; and
- Not present Mastercard or Maestro as a payment option less beneficial or useful than any other payment option.

Notwithstanding the foregoing, and for the avoidance of doubt, a Merchant located in the United States Region or a U.S. Territory may take any action set forth in Rule 5.12.1, "Discrimination," in the "Additional U.S. Region and U.S. Territory Rules" chapter; and a DWO in the United States Region or a U.S. Territory may also take any action that Rule 5.12.1 permits a Merchant in the United States Region or a U.S. Territory to take, if such action is taken at the request of a Merchant in the United States Region or a U.S. Territory from which a Transaction is being made.

9.1.2 Branding Requirements

Each Digital Activity Customer and Staged DWO must comply with all of the following:

Transparency

A Digital Wallet, or other user interface provided to a Cardholder by a Digital Activity Customer or Staged DWO must comply with the *Mastercard Branding Guidelines*. The *Mastercard Branding Guidelines* apply to the identification of a Mastercard or Maestro Account in a Digital Wallet, or other user interface provided to a Cardholder, whether or not that Account is the default Account each time the Cardholder interacts with the Account credential. The Mastercard Brand Mark, Mastercard Symbol, and the Maestro Brand Mark, as applicable, must be shown in each instance that a Cardholder interacts with the Account credential with the Digital Wallet or other user interface provided to such Cardholder by a Digital Activity Customer or Staged DWO.

Every user interface that pertains to a Cardholder's use or potential use of a Mastercard branded Account is subject to the Corporation's review and approval.

Account Selection—User Choice

A Digital Activity Customer or Staged DWO that allows a user to set a default payment account, must not engage in a practice that overrides, or has the effect of overriding, the user's choice.

Notwithstanding the foregoing, and for the avoidance of doubt, a Merchant located in the United States Region or a U.S. Territory may take any action set forth in Rule 5.12.1, "Discrimination," in the "Additional U.S. Region and U.S. Territory Rules" chapter; and a DWO in the United States Region or a U.S. Territory may also take any action that Rule 5.12.1 permits a Merchant in the United States Region or a U.S. Territory to take, if such action is taken at the request of a Merchant in the United States Region or a U.S. Territory from which a Transaction is being made.

9.1.3 Confidentiality and Information Security

Each Digital Activity Customer and Staged DWO must comply with all of the following:

Safeguards

A Digital Activity Customer and Staged DWO must maintain a comprehensive written information security program that complies with all requirements and includes technical, physical, and administrative or organizational safeguards designed to:

- Ensure the security and confidentiality of Personal Data;
- Protect against any anticipated threats or hazards to the security and integrity of Personal Data;
- Protect against any actual or suspected unauthorized Processing, loss, or acquisition of any Personal Data (a "Security Incident");
- Ensure the proper disposal of Personal Data; and
- Regularly test or otherwise monitor the effectiveness of the safeguards.

Security Incidents

Except to the extent prohibited by applicable law, each Digital Activity Customer or the Acquirer of an effected Staged DWO, must inform the Corporation in writing, and in accordance with the earlier of the notification date required by the Account Data Compromise Standards set forth in the *Security Rules and Procedures* or applicable law, of a DWO Security Incident or potential DWO Security Incident including, by way of example and not limitation:

- Any incident or breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed; and
- Any known security issue pertaining to the DWO Program that may result in such incidents.

Each DWO, or the Acquirer of an effected Staged DWO, must reasonably cooperate in all matters relating to Security Incidents.

Transaction Data

A Digital Activity Customer and Staged DWO must only use Transaction Data to initiate a Transaction in accordance with the Standards, and for no other purpose.

Confidentiality

A Digital Activity Customer and Staged DWO must not use information provided by the Corporation, nor disclose any such information except:

- On a need-to-know basis to the Digital Activity Customer or the Staged DWO staff, contractors, accountants, auditors, and legal counsel subject to written confidentiality restrictions or professional rules of conduct consistent with the confidentiality requirements herein;
- As may be required by any court process or governmental agency having or claiming jurisdiction over the Digital Activity Customer or the Acquirer of an effected Staged DWO, in which event the Digital Activity Customer or the Acquirer of an effected Staged DWO must

promptly provide written notice of such requirement to the Issuer of the Account credential and the Corporation, and when commercially reasonable, the Digital Activity Customer or the Acquirer of an effected Staged DWO must seek confidential treatment of such information by the court or agency.

9.1.4 Security

Each Digital Activity Customer and Staged DWO must comply with any applicable security specifications required by the Corporation, certification and testing procedures described in applicable program documentation, and any other such certification and testing as the Corporation may require from time to time.

Each Digital Activity Customer and Staged DWO must establish fraud loss controls satisfactory to the Corporation for each of its Programs and use them in accordance with the Standards.

9.2 DWO Requirements — Pass-through Digital Wallet

Each Pass-through DWO must operate a Pass-through Digital Wallet in accordance with the Standards as may be in effect from time to time.

9.2.1 Payment Card Industry Data Security Standard

Unless the Pass-through DWO is an Issuer, before offering a Pass-through Digital Wallet, the Pass-through DWO, using email to pcireports@mastercard.com, must certify its successful completion of an annual onsite assessment by a Payment Card Industry (PCI) Security Standards Council (SSC) approved Qualified Security Assessor (QSA) and the completion of quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV).

9.2.2 Prohibited Practices

A Pass-through DWO must not:

1. Inhibit or prevent
   a. A Merchant's choice as to which interfaces to support and must not require support for an alternate or proprietary interface as a substitute for, or prerequisite for enablement of, an industry-standard interface;
   b. A Mastercard or Maestro Account provisioned onto a near-field communication (NFC)-enabled Mobile Payment Device from being used to make payments at a contactless-enabled POS Terminal deployed at a Merchant;
   c. A Mastercard or Maestro Account provisioned onto a Mobile Payment Device from being used to make "in-application" purchases at a Merchant capable of processing Digital Secure Remote Payment Transactions; or
   d. A Mastercard or Maestro Account provisioned into a Pass-through Digital Wallet from being used to make in-browser purchases at a Merchant that is in compliance with applicable security Standards as may be amended from time to time.

2. Charge a Merchant any fee or other charge for the acceptance of Mastercard Account credentials by the Merchant. No other fee or charge can be assessed by a Pass-through DWO to a Merchant unless the Merchant and the Pass-through DWO agree otherwise.
3. Offer to provide any incentive that could have the effect of encouraging consumers to not use a Mastercard or Maestro Account as a default payment option, including, by way of example and not limitation, offering a direct or indirect reward or benefit for doing so.

Notwithstanding the foregoing in this Rule 9.2.2, and for the avoidance of doubt, a Merchant located in the United States Region or a U.S. Territory may take any action set forth in Rule 5.12.1, "Discrimination," in the "Additional U.S. Region and U.S. Territory Rules" chapter; and a DWO in the United States Region or a U.S. Territory may also take any action that Rule 5.12.1 permits a Merchant in the United States Region or a U.S. Territory to take, if such action is taken at the request of a Merchant in the United States Region or a U.S. Territory from which a Transaction is being made.

9.2.3 Industry-standard Interfaces

A Pass-through DWO must enable access to a Mastercard or Maestro Account credential stored in a Pass-through Digital Wallet using an industry-standard interface, as applicable in the relevant channel and as approved by the Corporation.

9.2.4 Pass-through DWO Tokenization

A Pass-through DWO must:

- Support a Mastercard Token; and
- Present a Mastercard Token if the Issuer, at the time of provisioning, Tokenized the Account.

9.2.5 Fraud Loss Controls and Account Data Compromise

Each Pass-through DWO is responsible to the Corporation and to all other Customers, including but not limited to those whose Cardholders may elect to enroll in any of its Pass-through Digital Wallet offerings, for all acts or omissions arising from the performance of its Pass-through Digital Wallets.

The Corporation may hold such Pass-through DWO or other Customers liable, in full or in part, pursuant to section 10.3, "Responsibilities in Connection with ADC Events and Potential ADC Events," of the *Security Rules and Procedures* manual, if the Corporation determines that the Pass-through DWO or other Customer's Digital Wallet, or any device, network, system, or environment employed in connection with the Pass-through Digital Wallet, was compromised, or vulnerable to compromise, or that the Pass-through DWO or other Customer has or had a direct or indirect relationship with an agent or other third party whose device, network, system, or environment was compromised or vulnerable to compromise.

9.2.6 Pass-through DWO Functional Requirements for Use on a Mobile Payment Device and Access Device

Each of the following, when required by the Corporation to be performed, must be performed in accordance with the Standards.

A Pass-through DWO must ensure that each Mobile Payment Device or Access Device used in connection with the Pass-through Digital Wallet can perform all of the following in accordance with the Corporation's minimum Standards:

1. Identification and Verification (ID&V), pursuant to a Token Implementation Plan deemed acceptable by the Corporation;
2. Device Binding;
3. Any form of Consumer Device Cardholder Verification Method (CDCVM);
4. Contactless Transactions, which may be supported in both Magnetic Stripe Mode and EMV Mode or in EMV Mode only; and
5. Digital Secure Remote Payment Transactions.

Device Binding

Each Pass-through DWO that proposes to conduct Device Binding for Mastercard Tokens must:

1. Be certified by the Corporation in accordance with the Global Vendor Certification Program (GVCP) as compliant with all applicable physical and logical security requirements for data preparation and mobile provisioning, as described in section 2.3, "Card Production Security Standards," of the *Security Rules and Procedures* manual;
2. Ensure that all transmissions to and from the Wallet Token Requestor are secured through a mutually authenticated Secure Sockets Layer (SSL; client and server authentication); and
3. Store encryption keys in a secure key management center, and use two-level or three-level key encryption hierarchy for encryption key management.

Consumer Device Cardholder Verification Method

A Pass-through DWO that enables Transactions on a Mobile Payment Device or other Access Device must only use a CDCVM qualified by the Corporation for use with a Mastercard Account credential. The CDCVM may include software, hardware, or a combination of the two in a particular application.

Each CDCVM supported or proposed to be supported on a Mobile Payment Device in connection with the use of a Pass-through Digital Wallet must be qualified by the Corporation prior to use by Cardholders. A Pass-through DWO is fully liable for Issuer fraud losses that result from the use of a non-Corporation-qualified CDCVM.

Issuer Authentication

Each Pass-through DWO that enables Transactions on a Mobile Payment Device or other Access Device must enable the Issuer of a Mastercard Account credential, stored in a Pass-through Digital Wallet, to authenticate or delegate the authentication of the Cardholder at the time of the Transaction, with an authentication method approved by the Corporation or as otherwise required by applicable law.

9.2.7 Pass-through DWO Token Requestor Requirements

A Pass-through DWO must comply with all of the following when requesting Tokenization of a Mastercard Account:

1. Adopt a standard Token Implementation Plan provided by the Corporation, or establish a Token Implementation Plan that is acceptable to the Corporation and complies with the Mastercard Digital Enablement Service Specifications or Mastercard Token Service Provider Standards, as applicable. For the avoidance of doubt, a Token Implementation Plan established with a Token Service Provider must be substantially similar in all material respects to a Token Implementation Plan used for the Mastercard Digital Enablement Service (MDES); and
2. For each Mastercard Token implementation, use ID&V Parameters that are equivalent to those set forth in the Token Implementation Plan, regardless of whether the Mastercard Digital Enablement Service will Digitize the Accounts, the Mastercard Token Vault will perform primary account number (PAN) mapping and cryptography validation of the Mastercard Tokens, or the Tokenization will be performed by a registered Token Service Provider.

A Wallet Token Requestor must comply with all of the following requirements:

1. Before MDES participation begins and on an ongoing basis thereafter, perform testing and obtain any necessary certifications of its equipment, procedures, and systems as the Corporation may require to ensure compatibility with its technical specifications then in effect, and ensure its capability to transmit all required Mastercard Token authorization request message data;
2. Register for the appropriate Tokenization Program; and
3. Use a Token solely for the purpose for which the Token was generated.

The Corporation reserves the right to approve, refuse to approve, require the modification of, or withdraw the approval of a Token Implementation Plan, and to suspend, either temporarily or permanently, a Wallet Token Requestor's MDES participation, in its sole discretion.

A Customer may submit a written request that the Corporation's Chief Franchise Officer review such action, provided the request is postmarked within 30 days of the date on which notice of the action was received, and is signed by the Customer's Principal Contact. Any decision by the Chief Franchise Officer is final and not subject to further review or other action.

9.2.8 Enablement of QR-based Payments

NOTE: A Rule on this subject appears in the "Latin America and the Caribbean Region" chapter.

9.3 Digital Activity—Merchant Token Requestor

A Merchant may apply to be a Digital Activity Customer approved for participation in a Merchant Card-on-File Tokenization Program.

No Merchant may directly participate in a Merchant Card-on-File Tokenization Program until approved by the Corporation to be a Digital Activity Customer, or as otherwise agreed by the Corporation. To be approved, such Merchant must execute the applicable Digital Activity Agreement in a form acceptable to the Corporation and pay all associated fees and other costs.

Participation in a Merchant Card-on-File Tokenization Program does not modify the rights and obligations of the Merchant Agreement between the Merchant and an Acquirer.

9.3.1 Merchant Token Requestor Requirements

A Mastercard or Maestro Account PAN provided by a Cardholder to a Merchant for the purpose of effecting a future Transaction with the Merchant may be Tokenized in accordance with a Merchant Card-on-File Tokenization Program.

A Mastercard or Maestro Account PAN Tokenized through the use of a Merchant Card-on-File Tokenization Program, must be Tokenized in accordance with the applicable standard Token Implementation Plan.

A Token generated in accordance with a Merchant Card-on-File Tokenization Program must only be used to effect a Transaction between the Cardholder that provided the PAN and the Merchant that requested Tokenization of the PAN.

A Merchant Token Requestor must comply with all of the following requirements:

1. Register to participate in a Merchant Card-on-File Tokenization Program.
2. Before beginning participation and on an ongoing basis thereafter, perform such testing and obtain any certifications of its equipment, procedures, and systems as the Corporation from time to time may require to ensure compatibility with technical specifications then in effect or for any other reason the Corporation deems necessary or appropriate.
3. Requirements set forth in the *Mastercard Branding Guidelines*.

The Corporation reserves the right to suspend or terminate a Merchant Token Requestor's participation in a Merchant Card-on-File Tokenization Program. A Customer may submit a written request that the Corporation's Chief Franchise Officer review such action provided the request is postmarked within 30 days of the date on which notice of the action was provided and is signed by the Customer's principal contact. Any decision by the Chief Franchise Officer is final and not subject to further review or other action.

9.3.2 Merchant Token Requestor Obligations

A Merchant Token Requestor must not offer to provide any incentive that could have the effect of encouraging consumers to not use a Mastercard or Maestro Account as a default payment option, including, by way of example and not limitation, offering a direct or indirect reward or benefit for doing so.

Notwithstanding the foregoing, and for the avoidance of doubt, a Merchant located in the United States Region or a U.S. Territory may take any action set forth in Rule 5.12.1, "Discrimination," in the "Additional U.S. Region and U.S. Territory Rules" chapter.

9.4 Digital Activity—On-behalf Token Requestor

An entity which proposes to connect directly or indirectly to the MDES for the purpose of requesting Tokens on behalf of a DWO or Merchant may apply to become an On-behalf Token Requestor in the On-behalf Tokenization Program.

No entity may directly participate as an On-behalf Token Requestor until such entity is approved by the Corporation to be a Digital Activity Customer, Service Provider, or as otherwise agreed by the Corporation. To be approved, such entity must execute the applicable Token Requestor agreement in a form acceptable to the Corporation and pay all associated fees and other costs.

9.4.1 On-behalf Token Requestor Requirements

An On-behalf Token Requestor must only Tokenize a Mastercard or Maestro Account PAN that it has received from a DWO or Merchant, subsequent to the DWO or Merchant having been provided the Account PAN by the authorized user of a Card with the intention that the PAN be stored for use in a future Transaction.

Tokens generated through the use of the On-behalf Tokenization Program must only be used to conduct a Transaction via the Digital Wallet for which a Token was generated (pursuant to the DWO's participation in the Pass-through Digital Wallet Tokenization Program), or between the Cardholder that provided the PAN and the Merchant that requested Tokenization of the PAN (pursuant to the Merchant's participation in the Merchant Card-on-File Tokenization Program). The On-behalf Token Requester is solely assigned all rights and responsibilities for the Tokens generated on behalf of the DWO or Merchant.

An On-behalf Token Requestor must comply with all of the following requirements:

1. Register and be approved for the On-behalf Tokenization Program;
2. Before participation begins and on an ongoing basis thereafter, perform testing and obtain any necessary certifications of its equipment, procedures, and systems as the Corporation may require to ensure compatibility with its technical specifications then in effect; and
3. Establish a Token Implementation Plan that is acceptable to the Corporation and complies with the Mastercard Digital Enablement Service Specifications.

The Corporation reserves the right to suspend or terminate an On-behalf Token Requestor's participation in the On-behalf Token Requestor Program. Such Participant may submit a written request that the Corporation's Chief Franchise Officer review such action provided the request is postmarked within 30 days of the date on which notice of the action was provided and is signed by such participant's principal contact. Any decision by the Chief Franchise Officer is final and not subject to further review or other action.

Before submitting a Tokenization request on behalf of a DWO or a Merchant, the On-behalf Token Requestor must:

1. Verify that the entity is operating a bona fide business, has sufficient safeguards in place to protect Account and Transaction Data from unauthorized disclosure or use, and complies with applicable laws;
2. Verify that the entity complies with the requirements set forth in the *Mastercard Branding Guidelines*;
3. Ensure that the entity complies with all Standards applicable to the Cardholder service provided (including, by way of example and not limitation, data use and protection, confidentiality and privacy Standards) for so long as such entity offers such Cardholder service, regardless of the nature of the Cardholder service offered; and
4. Ensure that the entity promptly provides to the Corporation any information requested by the Corporation pertaining to the use of the On-behalf Tokenization Program.

An On-behalf Token Requestor must not transfer or assign any part of its responsibilities or in any way limit its responsibility with regard to the use of the On-behalf Tokenization Program. An On-behalf Token Requestor must conduct meaningful monitoring of the entity for which the On-behalf Token Requestor Tokenizes an Account, to ensure ongoing compliance with the Standards.

Chapter 10 Payment Transfer Activity

This chapter contains Rules pertaining to Payment Transfer Activity (PTA) and PTA Customers.

Payment Transfer Activity Rules

Payment Transfer Activity (PTA) establishes a specific type of Customer, called a PTA Customer, that Participates in Payment Transfer Activity. Payment Transfer Activity involves a financial transaction in which funds are transferred from an Originating Institution to a Receiving Customer on behalf of Account Holders pursuant to a PTA Program. PTA Programs are types of Payment Transfer Activity and include the MoneySend Program, Mastercard Merchant Presented QR Program, and the Mastercard Gaming and Gambling Payments Program.

The Standards for PTA consist of these Rules (the "PTA Rules"); the PTA Agreement; and any other Standard that references Payment Transfer Activity or a PTA Program, PTA Customers, or PTA Transactions, each as amended from time to time.

This chapter applies to all Payment Transfer Activity, whether conducted pursuant to a PTA Agreement or License granted by the Corporation, or approved by the Corporation as set forth in a PTA Agreement or License granted, before or after the adoption of this chapter.

Applicability of Rules

The Rules in this Payment Transfer Activity chapter are variances and additions to the Rules in Chapters 1 through 9 that apply solely to Payment Transfer Activity.

The following Rules in Chapters 1 through 9 apply to Payment Transfer Activity (except as noted):

- Chapter 1 in its entirety, with the exception of Rules 1.8 The Digital Activity Agreement; 1.10 Participation in Competing Networks; and 1.11 Portfolio Sale, Transfer, or Withdrawal and its subsections
- Chapter 2 in its entirety
- Rule 3.2 Responsibility for Transactions
- Rule 3.3 Transaction Requirements
- Rule 3.4 Authorization Service
- Rule 3.7 Integrity of Brand and Network
- Rule 3.8 Fees, Assessments, and Other Payment Obligations and subsection 3.8.1 Taxes and Other Charges
- Rule 3.9 Obligation of Customer to Provide Information
- Rule 3.11 Use of Corporation Information by a Customer
- Rule 3.12 Confidential Information of Mastercard, including its subsection
- Rule 3.13 Privacy and Data Protection, including all subsections
- Rule 3.15 Cooperation
- Rule 3.17 BINs
- Rule 3.18 Recognized Currencies, including all subsections
- Rule 4.1 Right to Use the Marks, including all subsections except 4.1.1.1 Registration
- Rule 4.2 Requirements for Use of a Mark

- Rule 4.3 Review of Solicitations
- Rule 4.5 Use of the Interlocking Circles Device, including its subsection
- Rule 4.6 Use of Multiple Marks
- Rule 4.7 Particular Uses of a Mark, including all subsections except 4.7.9 Use on Cards
- Chapter 7 in its entirety, with the exception of Rules 7.2.7 Service Provider Identification on a Card; 7.6.7 Staged Digital Wallet Operator Requirements; and 7.7 Issuing Programs
- Rule 8.5 Failure of a Principal or Association to Discharge a Settlement Obligation
- Rule 8.9 Liability for Owned or Controlled Entities
- Rule 8.10 Risk of Loss
- Rule 8.12 PTA Transaction Settlement

10.1 All Participants Requirements

Each PTA Customer must comply with all of the following.

10.1.1 General Requirements

A PTA Customer must operate each of its PTA Programs in accordance with the Standards as may be in effect from time to time.

Each PTA Customer must provide, at its own expense and in compliance with the Standards, including but not limited to those set forth in the *Transaction Processing Rules* manual (if applicable) originating and/or receiving services with respect to any PTA Transaction in which the Sponsoring Customer and each of its Sponsored Affiliates has participated.

Each Payment Transfer Activity operated by a PTA Customer must:

- Avoid undue risk to the Corporation and its Customers; and
- Be operated in a manner that does not reflect poorly on the Corporation or any Mark.

Each PTA Customer represents and warrants throughout the entirety of its conduct of Payment Transfer Activity(ies) that such PTA Customer:

- Meets the eligibility criteria set forth in Rule 1.1.4 and any other Standards;
- Has all licenses, permits, registrations, and other governmental and local authority approvals and officially issued letters of approval or no-objection from governmental and local authorities, and satisfies all other requirements necessary for its Participation in the applicable PTA Program in accordance with applicable legal and regulatory requirements and Standards;
  - Ensures that its Service Providers and other agents (if any) that facilitate, initiate, receive, or otherwise provide services for PTA Transactions for or on behalf of such PTA Customer has all licenses, permits, registrations, and other governmental approvals, and satisfy all other requirements necessary for it to provide services in the applicable PTA Program in accordance with applicable legal and regulatory requirements and Standards;
  - Ensures that thorough anti-fraud and know your customer due diligence is conducted on each Account Holder and complies with all applicable laws and regulations and any

Standards related to anti-money laundering and economic sanctions for each PTA Transaction;

- Will not sponsor the Payment Transfer Activity of any Account Holder and will reject any PTA Transaction instruction that fails the checks described in the prior bullet and has an audit process to test such compliance; and
- If applicable, manages relationships between the PTA Customer and its Account Holders.

If a PTA Customer reasonably believes that an Account Holder may pose a higher risk to the integrity or the reputation of the Corporation or the Payment Transfer Activity and/or other Customers, the PTA Customer shall ensure that further due diligence and inquiries are carried out on such Account Holder. If the identified risks are not adequately addressed to the satisfaction of the PTA Customer or as required by applicable law or regulation or the Standards, the PTA Customer shall immediately stop sponsoring the Payment Transfer Activity for that Account Holder and shall notify the Corporation of the same, without prejudice to the Corporation's rights and remedies under these Rules or other Standards.

10.1.2 Branding Requirements

If applicable, each PTA Customer must comply with the branding guidelines applicable to each PTA Program in which the PTA Customer engages.

10.1.3 Transaction Limits

Each PTA Transaction will be subject to transaction limits (e.g., amount and velocity of PTA Transactions) as determined by the Corporation from time to time, as stated in the applicable Standards for a PTA Program, or if applicable, the Non-Mastercard Systems and Network Standards.

Each PTA Customer agrees to (a) enforce the transaction limits applicable to a PTA Transaction and (b) conduct value and velocity checks to confirm compliance with those limits.

The Corporation has the right, but not the obligation, to refuse to facilitate any PTA Transaction that exceeds the applicable transaction limits.

10.1.4 Use of PTA Service

Each PTA Customer shall integrate the PTA Program(s) that it Participates in with the applicable Corporation System(s) or as otherwise permitted by the Corporation, in compliance with the Standards. Each PTA Customer shall provide the information and instructions for each PTA Transaction as required by applicable law and regulation and pursuant to the Standards.

Each PTA Customer acknowledges and agrees that each PTA Transaction is subject to approval by the Receiving Customer and, if applicable, is governed by Non-Mastercard Systems and Network Standards. The posting of funds to a PTA Receiving Account is subject to such approvals, in addition to any other requirements set forth in these Rules and any Standards.

10.1.5 Non-Discrimination

A PTA Customer must not discriminate against any other PTA Customer with regard to the processing of any PTA Transaction unless otherwise permitted by the Standards or approved by the Corporation.

10.1.6 Security Incidents

Except to the extent prohibited by applicable law or regulation, each PTA Customer must provide notification to the Corporation (including using email to account_data_compromise@mastercard.com and for any Security Incident related to Personal Data, using a telephone to the Operations Command Center (OCC) at the Corporation at 1-636-722-6220 or 1-800-358-3060 and selecting the option to be directed to the Corporation's Security Operations Center) immediately upon identification that any Account Holder, individual, or entity has or potentially has materially breached the PTA Customer's security measures, or gained unauthorized access to any Personal Data held by the PTA Customer, and in particular of any incident or breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by the PTA Customer or is aware of any incident or potential incident of fraudulent PTA Transactions (any of the above, a "Security Incident"). Such notification must include all relevant information and evidence necessary to satisfy the Corporation. Upon any such discovery and among other actions, the PTA Customer must promptly investigate, remediate, and mitigate the effects of the Security Incident and provide the Corporation with information to reasonably assure the Corporation that such Security Incident will not recur.

The PTA Customer is solely responsible for providing any notices to Data Subjects as a result of any Security Incident, to the extent required by the Privacy and Data Protection Requirements.

The PTA Customer shall reasonably cooperate with the Corporation in all matters relating to Security Incidents and the PTA Customer acknowledges that it is responsible for any notices or remedial actions required by this Rule at its own cost and expense.

10.1.7 Disputes and Chargebacks

Each PTA Customer must comply with the Account Holder dispute provisions and chargeback provisions applicable to each PTA Program in which the PTA Customer engages.

10.1.8 Standards of Non-Mastercard Systems and Networks

Any Originating Institution originating PTA Transactions from a Non-Mastercard Funding Source, and to the extent permissible pursuant to the Standards applicable to a particular PTA Program, any Receiving Customer receiving to Non-Mastercard Receiving Accounts, only with respect to the portion of the PTA Transaction conducted on a Non-Mastercard System and Network, shall follow the Non-Mastercard Systems and Network Standards applicable to Non-Mastercard Funding Sources and/or Non-Mastercard Receiving Accounts as well as applicable laws and regulations, including but not limited to, with respect to any settlement, to transaction funds availability and/or velocity limitation requirements.

For the avoidance of doubt, the Standards do not apply to any portion of a PTA Transaction not conducted over a Mastercard network.

10.2 Originating Institution Requirements

Each PTA Customer that is an Originating Institution must comply with all of the following (and for the avoidance of doubt, when the PTA Originating Account is an Account, the Rules and Standards related to issuing and acquiring such an Account continue to apply).

10.2.1 Valid Transactions

An Originating Institution must only submit to the Corporation and a Receiving Customer valid PTA Transactions from a bona fide Originating Account Holder and only from funding sources that are permitted for the applicable PTA Program, and that are in compliance with applicable laws and regulations, Standards, and any Non-Mastercard Systems and Networks Standards.

An Originating Institution must not submit to the Corporation and/or a Receiving Customer a PTA Transaction that the Originating Institution knows or should have known to be fraudulent or not initiated by the Originating Account Holder, or that it knows or should have known to be initiated by an Originating Account Holder colluding with the Receiving Customer or the Receiving Customer's Receiving Account Holder for a fraudulent purpose. For purposes of this Rule, the Originating Institution is deemed to be responsible for the conduct of its employees, agents, and representatives.

An Originating Institution submitting a PTA Transaction on behalf of a business entity must verify that such PTA Transaction will be a bona fide business transaction.

10.2.2 Originating Institution Responsibilities to Originating Account Holders

An Originating Institution must ensure that each Originating Account Holder has agreed to participate as an Account Holder originating PTA Transactions.

Without limitation to the foregoing, such agreement must include appropriate provisions to govern such information, terms and conditions as necessary under applicable law and regulation and the Standards.

Each Originating Institution must ensure that each Originating Account Holder is provided with all necessary and appropriate information and disclosures in accordance with applicable laws and regulations and the Standards.

10.2.3 Limitation of Liability of Originating Account Holders for Unauthorized Use

Without prejudice to any applicable law or regulation, for any Mastercard or Maestro branded PTA Transactions and as otherwise set forth in the Standards, an Originating Institution must not hold an Originating Account Holder liable for any PTA Transaction that was not initiated by the Originating Account Holder if the Originating Account Holder exercised reasonable care in safeguarding the PTA Account from risk of loss or theft and, upon becoming aware of such loss or theft, promptly reported the loss or theft to the Originating Institution.

This Rule shall not apply to any such PTA Transaction conducted where the PTA Originating Account is:

1. Established by an entity other than a natural person or for a commercial purpose, except that the Rule shall apply to PTA Originating Accounts established for use by a small business; or
2. Established by and/or sold to a person until such time as that person's identity is registered by or on behalf of the Originating Institution in connection with such establishment and/or sale, which registration may include Originating Account Holder identification program requirements.

If applicable law or regulation imposes a greater liability or a conflicting obligation, such applicable law or regulation shall govern.

10.2.4 Sufficient Funds

Each Originating Institution shall ensure that an Originating Account Holder has sufficient funds available (which must include the total amount of the PTA Transaction and any fees imposed and may include an overdraft, whether pre-initiated or not) to complete each PTA Transaction prior to initiating each PTA Transaction.

10.2.5 Authentication

Each Originating Institution is responsible for:

- Authenticating each of its Originating Account Holders in respect of all PTA Transactions initiated by that Originating Account Holder, and rejecting any Originating Account Holder or PTA Transaction (as applicable) that fails such checks;
- Screening the PTA Originating Account and the PTA Receiving Account against the Mastercard Electronic Warning Bulletin (EWB); and
- With respect to a mobile or web-based PTA Program, authenticating the PTA Originating Account debiting funds and providing a secure way for the Originating Account Holder to access the service such as user ID/password authentication or biometrics.

In each case, the above must be done with the Originating Institution's usual compliance policies and procedures and all applicable laws and regulations and the Standards.

Each Originating Institution shall be liable for all losses arising from or in connection with any failure in the above.

10.2.6 Irrevocability and Discharge of Settlements

An Originating Institution cannot revoke, and shall become liable in respect of settlement of the amount of a PTA Transaction once the Originating Institution's system confirms or initiates, as applicable, a PTA Transaction to the Corporation, except as required or permitted by the Standards (the "Point of Irrevocability").

At the Point of Irrevocability, the Originating Institution becomes obligated to settle the amount of a PTA Transaction to the Receiving Customer in accordance with the Standards.

Each Originating Institution shall settle PTA Transactions in full without any withholding.

The Corporation subsequently creates instructions reflecting each Customer's net settlement obligations. Customers are required to effect funds transfers in accordance with these instructions, which result in the assumption or discharge of payment obligations between Customers.

For additional information regarding settlement finality and discharge of settlement obligations following an instruction, see the *Settlement Manual*.

10.3 Receiving Customer Requirements

Each PTA Customer that is a Receiving Customer must comply with all of the following.

10.3.1 Valid Transactions

A Receiving Customer must only accept PTA Transactions to a PTA Receiving Account type that is permitted for the applicable PTA Program.

10.3.2 Receiving Institution Responsibilities to Receiving Account Holders

A Receiving Institution must ensure that each Receiving Account Holder has agreed to participate as an Account Holder receiving PTA Transactions.

Without limitation to the foregoing, such agreement must include appropriate provisions to govern such information, terms and conditions as necessary under applicable law and regulation and the Standards.

Each Receiving Institution must ensure that each Receiving Account Holder is provided with all necessary and appropriate information and disclosures in accordance with applicable laws and regulations and the Standards.

10.3.3 Transaction Funds Availability

Each Receiving Customer is required to ensure that funds are made available to the Receiving Account Holder within the time period required by the applicable law or regulation, the Standards, or if applicable, the Non-Mastercard Systems and Networks Standards.

If applicable to a PTA Program, to the extent a Receiving Account Holder's PTA Receiving Account is not held at the Receiving Customer, the Receiving Customer is fully responsible and liable for delivering the funds transferred in the PTA Transaction to the Receiving Account Holder, as set forth in the Standards.

Chapter 11 Asia/Pacific Region

This chapter contains Rules pertaining to Activity conducted in the Asia/Pacific Region.

Applicability of Rules

The Rules in this Asia/Pacific Region chapter are variances and additions to the "global" Rules that apply in the Asia/Pacific Region or in a particular Region country or countries.

Rule 5.1.2, Rule 5.11.1 and Rule 5.11.2 in this Asia/Pacific Region chapter, as they apply in New Zealand, apply to Debit Mastercard Cards and Other Mastercard Cards (and not to Cirrus-only Cards or Maestro-only Cards) issued in New Zealand by New Zealand Customers and presented for payment at Merchant locations in New Zealand. Customers and Merchants in New Zealand must continue to comply with the global rules for Cards issued by Customers outside of New Zealand and presented for payment at Merchant locations in New Zealand.

Refer to Appendix A for the Asia/Pacific Region geographic listing.

Definitions

Solely within New Zealand, the following terms have the meanings set forth below:

Debit, Debit Mastercard Card, Debit Card

Any Mastercard Card or Program issued in New Zealand by a New Zealand Customer that when presented for payment in New Zealand, accesses, debits, holds, or settles funds from a consumer's demand deposit or asset account. "Debit" or "Debit Mastercard Card" shall include consumer signature debit programs, stored value programs, prepaid cards, payroll cards, electronic benefit transfer cards, and deferred debit cards that access, debit, hold, or settle funds from the user's demand deposit or asset account less than fourteen days after the date of purchase. "Debit" shall not include any Card or Program that accesses, debits, hold, or settles funds from the user's demand deposit or asset account 14 or more days after the date of the purchase.

Other Mastercard Card

Any Mastercard Card or Program issued in New Zealand by a New Zealand Customer that is not defined as "debit" or "Debit Mastercard Card."

1.7 Area of Use of the License

1.7.1 Extending the Area of Use

With respect to India, the Rule on this subject is modified as follows.

A License and written authorization from the Reserve Bank of India is required in order to conduct Activity in India.

1.7.2 Extension of Area of Use Programs

In Australia, the Rule on this subject is modified as follows.

A Mastercard Corporate Card® Card Program issued or distributed pursuant to paragraph 3 of Rule 1.7.2 by an Issuer whose Portfolio principally supports business-to-business payments must not include Cards issued outside of Australia for the express purpose of facilitating business-to-business payments to a supplier located in Australia, in connection with the provision of goods or services purchased by a consumer located in Australia.

1.10 Participation in Competing Networks

In the Asia/Pacific Region, the Rule on this subject is modified as follows

With the exception of Issuers in American Samoa, Guam, and Northern Mariana Islands, a Maestro Customer must not issue debit cards in any Competing PIN POS Network. A Maestro Customer, including a Customer in American Samoa, Guam, and Northern Mariana Islands, must not issue debit cards in any Competing International ATM Network.

3.1 Obligation to Issue Mastercard Cards

The Rule on this subject does not apply in New Zealand.

3.3 Transaction Requirements

In Mainland China, the Rule on this subject is modified as follows.

The China Switch allows a Customer to use China Dispute Resolution Platform to manually reverse or complete a domestic preauthorization and initiate the refund for a processed Mainland China domestic Transactions. The Standards in the Transaction Processing Rules that apply to preauthorization reversal, preauthorization completion or refund, apply to manual preauthorization reversal, manual preauthorization completion and manual refund of a Mainland China domestic Transaction.

A Chip Card issued in Mainland China capable of Mainland China domestic Transactions contains both PBoC and EMV standard applications. PBoC chip standards are Mainland China financial integrated circuit card specifications that follow EMV chip standards. The Standards applicable to a EMV card Transaction will also apply to a Mainland China domestic Transaction completed by a PBoC chip application.

Refer to the China Switch Specifications manual for technical requirements relating to Processed Transactions.

3.13 Data Protection

3.13.8 Regional Variances and Additions

A Customer that is subject to China Data Protection Law must comply with China Data Protection Law, Rule 3.13 as set forth in Chapter 3, "Customers Obligations", and this Rule 3.13.8, which applies to the Processing of Personal Data subject to China Data Protection Law.

As used in this Rule, the following terms have the meanings as described below.

Mainland China

The mainland of the People's Republic of China, for the avoidance of doubt, excluding the Hong Kong Special Administrative Region, the Macao Special Administrative Region and Taiwan.

China Data Protection Law

Any law, statute, declaration, decree, legislation, enactment, order, ordinance, directive, regulation or rule (as amended and replaced from time to time) promulgated by the relevant competent authorities in Mainland China which regulates the Processing of Personal Data to which the Customer (and where applicable, the Corporation) are subject in Mainland China, including but not limited to the Personal Information Protection Law of the People's Republic of China.

Controller

The entity (or individual) which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or other unauthorized Processing of Personal Data transmitted, stored, or otherwise Processed.

Processor

The entity (or individual) which Processes Personal Data on behalf of a Controller.

Sensitive Personal Data

Any Personal Data that is considered to be sensitive according to China Data Protection Law, including any Personal Data that, if leaked or illegally used, is likely to cause harm to a natural person's personal dignity or endanger a natural person's personal or property safety, such as Personal Data revealing biometrics, religious beliefs, particular capacity, medical treatments, health, financial accounts, tracks, etc., and Personal Data of minors under the age of 14.

Sub-Processor

The entity (or individual) engaged by a Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the relevant Controller(s).

3.13.8.1 Processing of Personal Data for Purposes of Activity and Digital Activity

In Mainland China, Rule 3.13.1 is modified to include the following.

A Customer is a Controller with regard to the Processing of Personal Data for the purposes of carrying out the Customer's Activities or Digital Activities, and the Corporation acts as a Processor for these purposes.

Each Customer acknowledges that the Corporation may Process, as a Controller, Personal Data for the purposes of accounting, auditing and billing; fraud, financial crime and risk management; defense against claims, litigation and other liabilities; arbitration and other decisions relating to dispute resolution; product development and improvement; internal research, reporting and analysis; anonymization of data to develop data analytics products; and compliance with legal obligations. The Corporation represents and warrants that the Corporation will Process Personal Data for these purposes in compliance with China Data Protection Law (where applicable) and the Standards.

To the extent that it acts as a Processor, the Corporation will: (1) cooperate with the Customers in their role as Controllers to fulfill their data protection compliance obligations in accordance with China Data Protection Law; (2) only undertake Processing of Personal Data in accordance with the Customer's instructions where they are in compliance with China Data Protection Law and the Standards and not for any other purposes or by other means than those specified in the Standards, the Customer's instructions, or as otherwise agreed in writing; and (3) adopt appropriate organizational, physical and security measures to safeguard the security of Personal Data Processed.

3.13.8.2 Data Subject Notice and Consent

In Mainland China, Rule 3.13.2 is modified to include the following.

A Customer must ensure that the Processing of Personal Data for the purposes provided in Rule 3.13.1 is based on a valid legal ground under China Data Protection Law, including obtaining Data Subjects' proper consent (including separate consent) where required or appropriate under China Data Protection Law, so that Personal Data (including Sensitive Personal Data, if any) relating to them may be collected, used, disclosed, transferred (including any overseas transfers) or otherwise Processed by the applicable Customer and the Corporation for the purposes set forth in the Standards.

A Customer must ensure that Data Subjects are provided with an appropriate notice with at the minimum all of the elements required under China Data Protection Law (including with respect to the Processing of Sensitive Personal Data and overseas transfers of Personal Data to the Corporation located outside of Mainland China, including Mastercard International Incorporated in the U.S.A., and Mastercard Asia/Pacific Pte. Ltd. in Singapore and other affiliates).

3.13.8.3 Data Subject Rights

In Mainland China, Rule 3.13.3 is modified to include the following.

A Customer must develop and implement appropriate procedures for handling Data Subjects' requests to exercise their rights under China Data Protection Law, including, as applicable, the right of (a) access, (b) rectification, (c) erasure, (d) data transfer, (e) restriction of Processing of Personal Data, (f) objection, (g) requesting for explanation regarding the rules as to the Processing of Personal Data, and (h) not being subject to a decision based solely on automated processing, including profiling, which materially affects such Data Subjects' rights and interests.

To the extent that the Corporation acts as a Controller or where required by China Data Protection Law, the Corporation will also develop and implement appropriate procedures for responding to such requests from Data Subjects.

To the extent that the Corporation acts as a Processor, the Corporation will inform the Customer of requests it directly receives from Data Subjects and the Customer shall be responsible for responding to such requests from Data Subjects.

3.13.8.4 Accountability

Taking into account the nature, scope, context, means, and purposes of Processing of Personal Data, as well as the impact on the rights and interests of Data Subjects and the security risks that are presented by the Processing of Personal Data, the Customer (and where required under China Data Protection Law, the Corporation) must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that Processing of Personal Data is performed in accordance with the Standards and China Data Protection Law, including, as applicable, by appointing a data protection officer, maintaining records of Processing of Personal Data, complying with the principles of Processing established in China Data Protection Law, and performing data protection impact assessments. To the extent that the Corporation acts as a Processor, the Corporation will cooperate with the Customer to ensure compliance with and to assist the Customer in fulfilling their own obligations under China Data Protection Law.

3.13.8.5 International Data Transfers

Each Customer authorizes the Corporation to transfer Personal Data Processed outside of Mainland China, to the extent permissible under, and in accordance with, China Data Protection Law.

Each Customer acknowledges that for the purposes of carrying out the Customer's Activity or Digital Activity, the Customer may transfer Personal Data subject to China Data Protection Law out of Mainland China to the Corporation located outside of Mainland China, to the extent permissible under, and in accordance with, China Data Protection Law and the applicable contractual requirements issued by the relevant competent authorities. Notwithstanding any other provisions under the Data Protection sections in the Standards to the contrary, the clauses under the applicable contractual requirements issued by the relevant competent authorities should be deemed as having been incorporated into this Rule 3.13.8.5 by reference. To the extent required by China Data Protection Law, each Customer shall (a) complete self-assessment to identify and assess if any security risks may arise from or in connection with the

cross-border transfer of Personal Data, and (b) pass the security assessment administered by the relevant competent authorities, in compliance with China Data Protection Law.

3.13.8.6 Sub-Processing

In Mainland China, Rule 3.13.6 is modified to include the following.

To the extent that the Corporation acts as a Processor, subject to any requirements under China Data Protection Law, the Customer gives a general authorization to the Corporation to use internal and external Sub-Processors on its behalf.

The Corporation requires its Sub-Processors, via a written agreement or written document of equivalent effect, to comply with the requirements of China Data Protection Law applicable to Sub-Processors, with the Customers' instructions and with the same obligations as are imposed on the Corporation by the Standards.

3.13.8.7 Security and Data Protection Audit

In accordance with the Standards and China Data Protection Law, each Customer (and where required under China Data Protection Law, the Corporation) must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate level of security, the Customer (and where required under China Data Protection Law, the Corporation) must take into account the nature, scope, context, means, and purposes of Processing of Personal Data, as well as the impact on the rights and interests of Data Subjects and the security risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed. The Customer (and where required under China Data Protection Law, the Corporation) shall also take into account the appropriate level of security in the event of a material change in (i) actual control; (ii) scope of business; or (iii) regulatory and legal environment of the residing country/region, that may impact the security of the data.

The Corporation and each Customer must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and as applicable Processes Personal Data in accordance with the Customer's instructions.

3.13.8.8 Data Retention; Deleting Personal Data

The Corporation will retain Personal Data for no longer than is necessary for the purposes for which the Personal Data are Processed, unless a longer retention period is required or allowed under applicable law.

Upon termination of the Processing services or upon request by the Customer (to the extent that the Corporation acts as a Processor), or upon expiry of retention period (whether the Corporation acting as a Controller or a Processor), the Corporation will delete, anonymize, or return (where applicable and feasible) such Personal Data it Processes, holds, retains or stores, unless applicable law prevents the Corporation from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case the Corporation will

protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore).

3.13.8.9 Personal Data Breaches

Where the Corporation acts as a Processor, and where required under China Data Protection Law, the Corporation will (a) inform the Customer, without undue delay, of a Personal Data Breach; and (b) provide reasonable assistance to the Customer in complying with its own obligations in respect of a Personal Data Breach (which may include to implement emergency response plan, notify the relevant competent authorities and affected Data Subjects of the Personal Data Breach (if required), and provide a smooth channel for Data Subjects to safeguard their rights and interests concerning Personal Data).

3.13.8.10 Liability for China Data Protection Law Violations

The Customer, as a Controller, is responsible for the actual damage caused by the Processing of Personal Data, which is in violation of the Data Protection sections in the Standards and China Data Protection Law.

To the extent that the Corporation acts as a Controller, it is responsible for the actual damage caused by the Processing of Personal Data, which is in violation of the Data Protection sections in the Standards and China Data Protection Law (to the extent applicable).

To the extent that the Corporation acts as a Processor, it will be liable for the damage caused by the Processing of Personal Data only where it has acted intentionally or out of gross negligence in regard to non-compliance with obligations under China Data Protection Law (to the extent applicable) specifically directed to Processors or with lawful instructions of the Controller Customer.

To the maximum extent permissible by applicable law, liability as between the Corporation (whether acting as a Controller or a Processor) and the Customer is limited to actual damage suffered, and in no event shall a party be liable to the other party or any third party for any loss of profits, revenue or goodwill, costs of procurement of substitute products or services, loss of interruption of business, loss of anticipated savings, or loss of data or any exemplary, punitive, consequential, expectancy, special, indirect or incidental damages of any kind.

To the extent that the Customer and the Corporation are held jointly and severally liable by the relevant competent authorities for any damage caused to a third party by the Processing of Personal Data, where the Corporation has paid full compensation for the damage suffered, it is entitled to claim back from the Customer involved in the same Processing of Personal Data that part of the compensation not attributable to the Corporation's intentional misconduct or gross negligence.

3.13.8.11 Applicable Law and Jurisdiction

Any clauses under the Mastercard Rules in relation to the Processing of Personal Data subject to China Data Protection Law (including the Rule 3.13 and the Rule 3.13.8, "Mainland China Data Processing Rules") shall be governed by and shall be construed in accordance with, the laws of Singapore.

Any dispute arising from or in connection with the Mainland China Data Processing Rules, including any question regarding its existence, validity or termination, shall first be referred to

the authorized representatives of the parties for amicable settlement. Any dispute which cannot be resolved by amicable discussions within thirty (30) days of referral shall be submitted to the Presidents (or equivalent) of the respective parties or their nominees for resolution. If the parties fail to resolve such dispute through good faith negotiations, such dispute shall be referred to and finally resolved by arbitration administered by the Singapore International Arbitration Centre (the SIAC) in accordance with the Arbitration Rules of the SIAC (the SIAC Rules) for the time being in force, which rules are deemed to be incorporated by reference in this Rule 3.13.8.11. The seat of the arbitration shall be Singapore. The tribunal shall consist of one (1) arbitrator. The language of the arbitration shall be English. Nothing in this Rule 3.13.8.11 shall preclude a party from resorting to any court of competent jurisdiction for interim or interlocutory injunctive relief.

A person or entity who is not a party to the Mainland China Data Processing Rules shall have no right under the Contracts (Rights of Third Parties) Act, Chapter 53B to enforce any term of the Mainland China Data Processing Rules.

4.9 Use of Marks on Mastercard Cards

In Australia, the Rule on this subject is modified as follows.

The EFTPOS acceptance mark may appear only on the back of Mastercard Cards issued in Australia that provide access to a deposit account at the time of issuance.

When appearing on the back of a Mastercard Card, the EFTPOS acceptance mark is limited to acceptance solely within Australia. See the Card Design Standards for information regarding the placement of the EFTPOS acceptance mark on a Mastercard Card.

5.1 The Merchant and ATM Owner Agreements

5.1.2 Required Merchant Agreement Terms

In New Zealand, the Rule on this subject is modified as follows.

A Merchant Agreement for Mastercard Card acceptance must provide the Merchant with the options, and the applicable Merchant discount rate for each option, to elect to accept Debit Mastercard Cards only, Other Mastercard Cards only, or both Debit Mastercard Cards and Other Mastercard Cards. A Merchant may choose to stop accepting Debit Mastercard Cards or Other Mastercard Cards by providing no less than 30 days advance written notice to its Acquirer.

5.4 Acquirer Obligations to Merchants

5.4.2 Supplying Materials

In Singapore, the Rule on this subject is modified as follows.

If an Acquirer offers a Merchant located in Singapore the option of Singapore Quick Response (SGQR) as a method of receiving payments, then the Acquirer must participate in Mastercard Merchant-presented QR (MPQR) as a Receiving Institution and provide the Merchant with a QR code capable of carrying the Mastercard payload (static or dynamic) for Mastercard Merchant-presented QR payments, in accordance with the EMV QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode standard.

This requirement applies to any Acquirer that becomes an MPQR Receiving Institution on or after 15 July 2022, as well as to the Acquirers who have been Licensed by Mastercard and commence the Licensed Activity after 15 July 2022 and to all Acquirers as of 20 October 2023.

5.11 Merchant Obligations for Acceptance

5.11.1 Honor All Cards

In New Zealand, the Rule on this subject as it applies to Mastercard acceptance is replaced with the following:

1. **Honor All Debit Mastercard Cards**. Subject to Rule 5.12.1 in this Asia/Pacific Region chapter, a Merchant that chooses to accept Debit Mastercard Cards must honor all valid Debit Mastercard Cards without discrimination when properly presented for payment. Merchants must maintain a policy that does not discriminate among customers seeking to make purchases with a Debit Mastercard Card.
2. **Honor All Other Mastercard Cards**. Subject to Rule 5.12.1 in this Asia/Pacific Region chapter, a Merchant that chooses to accept Other Mastercard Cards must honor all Other Mastercard Cards without discrimination when properly presented for payment.

A Merchant must maintain a policy that does not discriminate among customers seeking to make purchases with Other Mastercard Cards.

5.11.2 Merchant Acceptance of Mastercard Cards

In New Zealand, a Merchant that accepts Mastercard Cards may choose to accept Debit Mastercard Cards only, Other Mastercard Cards only, or both Debit Mastercard Cards and Other Mastercard Cards.

An Acquirer must advise the Corporation when a New Zealand Merchant chooses not to accept either Debit Mastercard Cards or Other Mastercard Cards. An Acquirer must provide a complete list of accurate and current BINs obtained through the Corporation that apply to Debit Mastercard Cards to its Merchants and ensure that its Merchants use the updated BIN information within six calendar days of such file being made available by the Corporation.

5.11.5 Discounts or Other Benefits at the Point of Interaction

In the Asia/Pacific Region, a discount or other benefit may be applied by a Merchant at the POI upon presentation of a particular Mastercard Card for payment.

Promotion of any such discount or other benefit at the POI is permitted provided such promotion does not result in discrimination against other Mastercard Card Programs. The determination of whether any promotion discriminates against other Card Programs is at the sole discretion of the Corporation.

5.12 Prohibited Practices

5.12.1 Discrimination

In New Zealand, the Rule on this subject is modified as follows.

The Corporation will not consider steering at the point of sale by offering discounts, promotions, or financial incentives to encourage an alternate form of payment (including as between Cards and EFT POS cards, or cards from different schemes, or different types of Cards) of itself to constitute a breach of Rule 5.12.1 or any other Rule. Further, the Corporation will not consider Merchant surcharging pursuant to Rule 5.12.2 of this chapter to constitute a breach of Rule 5.12.1.

5.12.2 Charges to Cardholders

In Australia and New Zealand, the Rule on this subject is modified as follows, with respect to Mastercard POS Transactions. For all other Transactions, the global Rule applies.

The Rule on this subject does not apply to Australia or New Zealand. If a Merchant in Australia or New Zealand applies a surcharge for payment with a Mastercard Card, the amount or method of calculation of the surcharge must be clearly indicated to the Cardholder at the POI location and must bear a reasonable relationship to the Merchant's cost of accepting the Cards.

6.1 Card Issuance—General Requirements

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

All newly issued or re-issued Cards with contact and/or contactless chip functionality must be EMV-compliant.

In Mainland China, all newly issued or re-issued Cards with contact and/or contactless chip functionality must be PBoC and EMV-compliant.

Transaction Alerts Service

In the Asia/Pacific Region, the Issuer's offering of a Transaction alerts service is required for commercial Cards issued for use by a small or mid-sized business (as defined by the Corporation).

These requirements do not apply to an Issuer in Australia or New Zealand.

Mastercard Decision Intelligence

In Japan, the Rule on this subject is modified as follows.

Each Customer must participate in Mastercard Decision Intelligence.

Mastercard Acquirer Fraud Dashboard

In Japan, the Rule on this subject is modified as follows.

Each Acquirer must participate in Mastercard Acquirer Fraud Dashboard.

Mastercard Crypto Secure

The Rule on this subject does not apply to Issuers in Australia, China, India, Japan, New Zealand, and the Pacific Islands (American Samoa, Christmas Islands, Cocos (Keeling) Islands, Cook Islands, Fiji, French Polynesia, Guam, Heard and McDonald Islands, Kiribati, Marshall Islands, Micronesia, Nauru, New Caledonia, Niue, Norfolk Island, Northern Mariana Islands, Palau, Papua New Guinea, Pitcairn, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, U.S. Minor Outlying Islands, Vanuatu, Wallis and Futuna).

Mastercard Safety Net

In the Asia/Pacific Region, the requirement for Issuers to participate in Mastercard Safety Net or Mastercard Safety Net alerts for non-Processed Transactions does not apply.

6.1.1 Mastercard Card Issuance

In New Zealand, the Rule on this subject is modified as follows.

A Customer must use specific and unique bank identification numbers (BINs) for Debit Mastercard Cards. Refer to Rule 3.17 for more information.

6.1.4 Tokenization of Accounts

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

An Issuer must support Tokenization of all of its Accounts by a Token Service Provider initiated by a Token Requestor such as a mobile Payment Application offered by an Issuer or a Digital Wallet Operator or an e-commerce Merchant.

6.1.6 Enablement of QR-based Payments

In Singapore, an Issuer that offers Cardholders a mobile application capable of scanning Singapore QR (SGQR) codes must:

- Participate in Mastercard Merchant-presented QR (MPQR);

- Ensure the mobile application can scan and parse a QR code containing Mastercard payload information, in accordance with the EMV QR Code Specification for Payment Systems (EMV QRCPS) standard; and
- Offer Cardholders the option to select a Card as a source of funds for any QR-based payments.

This requirement applies to any Card Issuer that becomes an MPQR Originating Institution on or after 15 July 2022 and to all Card Issuers as of 20 October 2023.

8.3 Interchange and Service Fees

In New Zealand, the Rule on this subject is modified as follows.

Intracountry Mastercard Transactions are excluded from the list of Transactions for which the Corporation may establish default interchange and service fees.

8.4 Establishment of Intracountry Interchange and Service Fees

Rule 8.4 of this Asia/Pacific Region chapter, as it applies to Intracountry Mastercard Transactions occurring within New Zealand is replaced in its entirety with the following:

The Corporation will establish and publish on its website containing content specific to New Zealand and in such other manner as the Corporation deems appropriate, maximum interchange fees for all Intracountry Transactions (herein, the "Mastercard maximum interchange fee"). Each Issuer and Acquirer may negotiate bilateral interchange fees (subject to any Mastercard maximum interchange fee) and each Issuer may determine interchange fees applicable to its Intracountry Transactions (subject to any bilateral agreements and subject to any Mastercard maximum interchange fee). An Issuer must ensure that with respect to each of its Intracountry Transactions, neither a negotiated bilateral interchange fee nor an interchange fee set by the Issuer results in an interchange amount with respect to that Intracountry Transaction that exceeds the interchange amount payable pursuant to the maximum interchange fee set by the Corporation.

An Issuer must promptly notify the Corporation of the interchange fees applicable to its Intracountry Transactions. Such fees must not exceed the maximum interchange fee set by the Corporation. If an Issuer does not provide the Corporation with an interchange fee that applies to each of its Intracountry Transactions, then the Corporation will process the Transaction on the basis of a zero interchange fee.

Each Issuer must publish the intracountry interchange fees notified to the Corporation on its website except for those interchange fees which are subject to a bilateral agreement. The Corporation either will publish on its website containing content specific to New Zealand the Issuer's intracountry interchange fees (except for those interchange fees which are subject to a bilateral agreement) or will provide a link from its website to the relevant page of the Issuer's website.

8.4.1 Intraregional Fees

In New Zealand, the Rule on this subject is modified to exclude intraregional or interregional fees from applying by default to Intracountry Transactions. For the avoidance of doubt, the global Rule applies to Intracountry Mastercard Manual Cash Disbursement Transactions.

8.4.2 Bilateral Agreement

In the Asia/Pacific Region, the Rule on this subject is modified as follows.

All interchange fees applicable to Intracountry Transactions contained in a bilateral agreement must not exceed the maximum interchange fee set by the Corporation (the "Mastercard maximum interchange fee").

Chapter 12 Canada Region

This chapter contains Rules pertaining to Activity conducted in the Canada Region.

Applicability of Rules

The Rules in this Canada Region chapter are variances and additions to the "global" Rules that apply in the Canada Region.

Customers and Merchants must continue to comply with the global Rules with respect to Cards issued by Customers outside of the Canada Region and presented for payment at Merchant locations in the Canada Region, unless otherwise agreed by the Corporation.

All Customers must comply with the Code of Conduct for the Credit and Debit Card Industry in Canada (the "Code of Conduct"), including any Compliance Bulletins, Commissioner's Guidances, guidelines, attestation forms and/or expectations published, distributed or released by the Financial Consumer Agency of Canada ("FCAC") and/or Mastercard from time to time. Each Customer agrees that Mastercard may interpret the Code of Conduct in accordance with any published interpretation bulletins or guidance issued by the FCAC.

All Customers must ensure that all participants for which they are responsible, including participants that interact directly or indirectly with Merchants or Cardholders on behalf of the Customer, comply with the Code of Conduct.

Refer to Appendix A for the Canada Region geographic listing.

5.1 The Merchant and ATM Owner Agreements

5.1.2 Required Merchant Agreement Terms

5.1.2.1 Gambling Merchants

In the Canada Region, the Rule on this subject is modified as follows.

A Merchant may load winnings, unspent chips, or other value usable for gambling to a prepaid Card by means of a value load provided:

- It is consented to by the Issuer; and
- The load is not routed or processed through the Interchange System.

A Payment Transaction must not be processed to a prepaid Card with respect to gambling winnings, unspent chips, or other value usable for gambling.

5.4 Acquirer Obligations to Merchants

5.4.4 Merchant Deposit Account

The Acquirer of a Canada Region Merchant must have a deposit account for the Merchant and must deposit the proceeds of Mastercard POS Transactions submitted by the Merchant into the Merchant's deposit account.

5.8 Transaction Message Data

5.8.1 Card Acceptor Business Code (MCC) Information

In the Canada Region, the Rule on this subject is modified as follows.

A Canada Region Acquirer must use MCC 5912 (Drug Stores, Pharmacies) to identify Transactions arising from a Canada Region Merchant or Submerchant whose primary business involves the legal sale of recreational cannabis.

For a Canada Region Merchant or Submerchant whose primary business is not the sale of recreational cannabis, the MCC of the Merchant's or Submerchant's primary business must be used.

The Acquirer must register both such Merchant or Submerchant with the Corporation as described in section 9.4.7 of the *Security Rules and Procedures* manual.

5.11 Merchant Obligations for Acceptance

5.11.5 Discounts or Other Benefits at the Point of Interaction

The use of a Mastercard Card issued pursuant to an Affinity or Co-Brand Card Program to activate a discount or other benefit at the POI that is not available on similar purchases with the use of any other Mastercard Card is permitted for Intraregional Transactions effected in the Canada Region.

The determination of whether any such discount or other POI benefit practice complies with the Standards is at the sole discretion of the Corporation.

5.12 Prohibited Practices

5.12.2 Charges to Cardholders

In the Canada Region, the Rule on this subject is modified as follows.

In addition to a discount for cash, a Merchant may provide a discount to its customers for other forms of payment, including differential discounts for other payment brands. Such discounts must be clearly communicated at the Point of Interaction.

Effective 6 October 2022, in the Canada Region, the Rule on this subject is modified as follows, with respect to Mastercard Credit Card Transactions, as the term Mastercard Credit Card Transaction is defined herein. For all other Transactions, the global Rule applies.

Definitions

Solely for the purposes of Rule 5.12.2 in this Canada Region chapter, the following terms have the meanings set forth below:

1. "Cardholder" means the authorized user of a Mastercard Credit Card.
2. "Competitive Credit Card Brand" includes the brand of Credit Card or electronic credit payment form of the following payment networks: American Express and PayPal.
3. "Credit Card" means a card or other device that may be used to defer payment of debt or incur debt and defer its payment.
4. The "Effective Merchant Discount Rate" is calculated as the total fees paid by the Merchant to an Acquirer, related to the processing of a specific type of payment card from a payment card network, divided by the total sales volume for that type of payment card.
5. "Mastercard Credit Card" means a Credit Card bearing the Mastercard brand.
6. "Mastercard Credit Card Transaction" means a Transaction in which a Mastercard Credit Card is presented for payment and that is performed in accordance with the Standards.
7. The "Maximum Surcharge Cap" shall be the lesser of (i) 2.4%; or (ii) 1% plus Mastercard's average annual effective rate of interchange for credit card Transactions in Canada as set out in any voluntary or mandatory commitment to a Canadian governmental entity or otherwise reasonably determined by Mastercard if not so regulated, expressed as a percentage of Transaction value.
8. "Surcharge" means any fixed value or ad valorem fee charged by the Merchant for use of a Mastercard Credit Card. As set forth in this Rule 5.12.2 in this "Canada Region Rules," a Merchant located in the Canada Region may only require a Mastercard Credit Card Cardholder to pay a Surcharge by choosing to apply either, but not both, of the following Surcharge methods:
    a. Brand-level Surcharge—The application of the same Surcharge to all Mastercard Credit Card Transactions regardless of the Issuer.
    b. Product-level Surcharge—The application of the same Surcharge to all Mastercard Credit Card Transactions of the same product type regardless of the Issuer.

General Requirements

The following requirements apply to a Merchant that chooses to impose a Surcharge at the brand level or at the product level:

1. A Merchant that wishes to Surcharge a Mastercard Credit Card Transaction is prohibited from applying a Surcharge at the Issuer level.
2. A Merchant that wishes to Surcharge a Mastercard Credit Card Transaction is prohibited from applying a Surcharge if the Credit Card Transaction already attracts convenience fees or service fees as permitted by Rule 5.12.2.
3. Third party agents are not permitted to surcharge Mastercard Credit Card Transactions.
4. A Merchant may not impose a Surcharge on a Mastercard Credit Card Transaction (whether at the Brand-level or at the Product-level) at any higher percentage rate (or flat fee equivalent) than the Merchant imposes on transactions effected by use of any Competitive Credit Card Brands which Merchant accepts to effect payment. If the Merchant does not accept payment by any Competitive Payment Card Brand then this provision shall not apply to it unless or until the Merchant begins to accept payment by means of a Competitive Credit Card Brand.

5.12.2.1 Brand-level Surcharging

Definitions

Solely for purposes of this Rule 5.12.2.1, the following terms have the meanings set forth below:

1. "After accounting for any discounts or rebates offered by the Merchant at the Point of Interaction (POI)" means that the amount of the Surcharge for a Mastercard Credit Card or a Competitive Credit Card Brand is to include the amount of any discount or rebate that is applied to that card or brand at the POI but which is not equally applied to all Mastercard Credit Card Transactions.
2. "Mastercard Brand-level Surcharge Cap" is the Merchant's average Effective Merchant Discount Rate applicable to Mastercard Credit Card Transactions at the Merchant for the preceding one or twelve months, at the Merchant's option.

The following requirements apply to a Merchant that chooses to impose a Surcharge at the brand level:

1. The same Surcharge must apply to all Mastercard Credit Card Transactions after accounting for any discounts or rebates offered by the Merchant on Mastercard Credit Card Transactions at the POI. However, a Merchant may choose to Surcharge:
   a. all face-to-face Mastercard Credit Card Transactions, but not non-face-to-face Mastercard Credit Card Transactions, or
   b. all non–face-to-face Mastercard Credit Card Transactions, but not face-to-face Mastercard Credit Card Transactions, or
   c. all face-to-face and all non-face-to-face Mastercard Credit Card Transactions.
2. The Surcharge assessed on a Mastercard Credit Card Transaction may not exceed the lesser of:
   a. The Merchant's Mastercard Brand-level Surcharge Cap, or
   b. The Maximum Surcharge Cap, as published by Mastercard from time to time.
3. The Merchant must comply with the Surcharge disclosure requirements set forth in Rule 5.12.2.3 below.

5.12.2.2 Product-level Surcharging

Definitions

Solely for purposes of this Rule 5.12.2.2, the following terms have the meanings set forth below:

1. "After accounting for any discounts or rebates offered by the Merchant at the POI" means that the amount of the Surcharge for Mastercard Credit Cards of the same Product Type or a Competitive Credit Card Product is to include the amount of any discount or rebate that is applied to that card or product at the POI but which is not equally applied to all Mastercard Credit Card Transactions of the same Product Type.
2. The "Mastercard Product-level Surcharge Cap" for a Mastercard Product Type is the average Effective Merchant Discount Rate applicable to Mastercard Credit Card Transactions of that Product Type at the Merchant for the preceding one month or twelve months, at the Merchant's option.

3. "Product Type "refers to Standard Mastercard, World Mastercard, World Elite Mastercard, Muse Mastercard and any potential similar future product Mastercard Credit Card constructs as defined by Mastercard from time to time.

The following requirements apply to a Merchant that chooses to impose a Surcharge at the product level:

1. The same Surcharge must apply to all Mastercard Credit Card Transactions of the same Product Type (for example, Standard Mastercard, World Mastercard, World Elite Mastercard, Muse Mastercard) after accounting for any discounts or rebates offered by the Merchant at the POI. A Merchant may choose to surcharge:
   a. all face-to-face Mastercard Credit Card Transactions of the same Product Type, but not non-face-to-face Mastercard Credit Card Transactions of the Product Type, or
   b. all non–face-to-face Mastercard Credit Card Transactions of the same Product Type, but not face-to-face Mastercard Credit Card Transactions of the same Product Type, or
   c. all face-to-face and all non–face-to-face Mastercard Credit Card Transactions of the same Product Type.
2. The Surcharge assessed on a Mastercard Credit Card Transaction may not exceed the lesser of:
   a. The Merchant's Mastercard Product-level Surcharge Cap for that Product Type, or
   b. The Maximum Surcharge Cap, as published by Mastercard from time to time.
3. The Merchant must comply with the surcharge disclosure requirements set forth in Rule 5.12.2.3 below.

5.12.2.3 Requirements for Merchant Disclosure of a Surcharge at the POI

1. A Merchant that chooses to Surcharge, either at the brand level or at the product level, must prominently display a clear disclosure of the Merchant's Surcharge policy at all points 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 Effective 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 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, not by Mastercard; and
   c. A statement that the Surcharge is not greater than the applicable Merchant Discount Rate for Mastercard Credit Card Transactions at the Merchant.

   Cardholders must have the opportunity to cancel or opt-out of the Transaction upon disclosure of the Surcharge.
3. A Merchant that chooses to Surcharge must provide clear disclosure of the Surcharge amount (in dollars) on the Transaction receipt.

5.12.2.4 Merchant Notification

A Merchant that chooses to impose a Surcharge must provide Mastercard and its Acquirer with no less than 30 days' advance written notice that the Merchant intends to impose a Surcharge on Mastercard Credit Card Transactions at either the brand level or product level.

For information about how to notify Mastercard, see www.mastercard.ca/surchargedisclosure.

5.12.2.5 Transaction Requirements

A Merchant that applies a Mastercard Brand-level Surcharge or a Mastercard Product-level Surcharge must disclose the Surcharge amount (in dollars) on the Transaction Information Document (TID) set forth set forth in Rule 5.12.2.3.

In the event that a Merchant provides a full or partial refund of a purchase Transaction that included a Mastercard Brand-level Surcharge or a Mastercard Product-level Surcharge, the refund Transaction must include the full or prorated Mastercard Brand-level Surcharge or Mastercard Product-level Surcharge amount.

6.1 Card Issuance—General Requirements

Transaction Alerts Service

An Issuer in the Canada Region must comply with the Transaction alerts service requirements set forth in Rule 6.1 of Chapter 6. The Issuer's offering of a Transaction alerts service is required for commercial Cards issued for use by a small or mid-sized business (as defined by the Corporation).

Mastercard Safety Net

In the Canada Region, the requirement for Issuers to participate in Mastercard Safety Net or Mastercard Safety Net alerts for non-Processed Transactions does not apply.

6.1.1 Mastercard Card Issuance

In the Canada Region, the Rule on this subject is modified as follows.

An Issuer must ensure that each contactless-enabled Mastercard Card and Access Device is personalized with the appropriate device type value.

6.1.2 Maestro Card Issuance

In the Canada Region, the Rule on this subject is modified as follows.

When an Issuer issues a Maestro Card that contains the Maestro Brand Mark and any other POS debit mark, the Issuer must not prioritize Maestro on the Financial Institution Table (FIT).

6.10 Prepaid Card Programs

6.10.6 Value Loading

In the Canada Region, the Rule on this subject is modified as follows.

Value loads arising from gambling winnings, unspent chips or other value usable for gambling, or winnings related to a lottery scheme conducted and managed by a Canadian provincial government body, are permitted provided that:

- Value loads of winnings are not prohibited by applicable law or regulation;
- The Card is a consumer Card;
- The Customer complies with the requirements set forth in Rule 6.10; and
- The Card is not an anonymous prepaid Card, unless the value load is CAD 500 or less and represents winnings related to a lottery scheme conducted and managed by a Canadian provincial government body.

7.2 The Program and Performance of Program Service

In the Canada Region, the Rule on this subject is modified as follows.

A Canada Region Customer that performs services to effect the payment of an outstanding balance on a Mastercard Account issued by another Canada Region Customer for or on behalf of such Customer's Cardholder is deemed not to be a Service Provider of such Customer.

7.6 Acquiring Programs

7.6.7 Staged Digital Wallet Operator Requirements

In the Canada Region, the Rule on this subject is modified as follows:

MCC 6540 may not be used for a funding stage Transaction if such funds may subsequently be used for any of the following purposes; in such event, the funds must be segregated and used by the consumer solely for the designated purpose:

- The purchase of chips or other value usable for gambling (MCC 7801, MCC 7802, or MCC 7995 must be used);
- The purchase of access to adult content and services (MCC 5967 must be used);
- The purchase of any prescription drug (MCC 5122 or MCC 5912 must be used);
- The sale of any tobacco product (MCC 5993 must be used);
- The purchase of high-risk cyberlocker services (MCC 4816 must be used); or
- The purchase of recreational cannabis (MCC 5912 must be used for a Canada Region Merchant or Submerchant whose primary business involves the legal sale of recreational cannabis. For a Canada Region Merchant or Submerchant whose primary business is not the

sale of recreational cannabis, the MCC of the Merchant's or Submerchant's primary business must be used).

Chapter 13 Europe Region

This chapter contains Rules pertaining to Activity conducted in the Europe Region.

Applicability of Rules

The Rules in this Europe Region chapter are variances and additions to the "global" Rules that apply in the Europe Region or in a particular country or countries.

Rules 5.11.1, 5.11.2, and 6.1.1 apply to:

1. Debit Mastercard Cards issued in a Debit Mastercard Country and presented for payment in the Europe Region;
2. Debit Mastercard POS Transactions that take place in the Europe Region; and
3. Merchants and Acquirers of those Transactions.

The rules set forth in chapters 2 through 6 of the *UK Domestic Rules* manual also apply to Transactions effected with a Debit Mastercard Card that take place wholly within the United Kingdom.

Customers and Merchants that accept Debit Mastercard Cards must continue to comply with the global Rules with respect to all Mastercard Cards issued by Customers outside of the Europe Region and presented for payment at Merchant locations in the Europe Region, unless otherwise agreed by the Corporation.

Refer to Appendix A for the Europe Region, Non-Single European Payments Area (Non-SEPA) and Single European Payments Area (SEPA) geographic listings.

Definitions

Solely within the Europe Region, the following terms have the meanings set forth below:

Business Card

In Serbia, this term has the meaning set out in Serbian Law No. 44/2018.

Commercial Card

In the EEA, Gibraltar, and the United Kingdom this term has the meaning set out in EU Regulation 2015/751.

In Serbia, this term has the meaning set out in Serbian Law No. 44/2018.

In Bosnia and Herzegovina, this term has the meaning set out in Law on Interchange Fees for Card-Based Payment Transactions of Republika Srpska.

Credit Card, Credit Card Transaction

In the EEA, Gibraltar, and the United Kingdom these terms have the meaning set out in EU Regulation 2015/751 and the Interchange Fee (Amendment) (EU Exit) Regulations 2019.

In Serbia, these terms have the meaning set out in Serbian Law No. 44/2018.

In Bosnia and Herzegovina, these terms have the meaning set out in Law on Interchange Fees for Card-Based Payment Transactions of Republika Srpska.

Debit Card, Debit Card Transaction

In the EEA, Gibraltar, and the United Kingdom these terms have the meaning set out in EU Regulation 2015/751 and the Interchange Fee (Amendment) (EU Exit) Regulations 2019.

In Serbia, these terms have the meaning set out in Serbian Law No. 44/2018.

In Bosnia and Herzegovina, these terms have the meaning set out in Law on Interchange Fees for Card-Based Payment Transactions of Republika Srpska.

Debit Mastercard Card

If issued in the EEA, a Mastercard-branded Debit Card or Commercial Card, as "Debit Card" and "Commercial Card" are defined in this section. In all Europe Region countries, a Mastercard Card offering credit facilities for which the Cardholder has to enter into a written credit agreement with the Card issuing institution that would qualify as consumer credit under the applicable legislation governing consumer credit is not covered by this definition of Debit Mastercard Card. Overdraft facilities may be provided on an Account to which a Debit Mastercard Card is linked.

Debit Mastercard Country

A country designated by the Corporation, in its sole discretion, as a participant in the Intracountry Debit Mastercard Program. The following countries are Debit Mastercard Countries: Albania, Austria, Azerbaijan, Belgium, Bosnia, Bulgaria, Cyprus, Czech Republic, Croatia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Kazakhstan, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tajikistan, Turkey, Ukraine, and United Kingdom.

European Economic Area (EEA)

The following countries, islands, and territories: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Canary Islands, Ceuta, Melilla, Azores, Madeira, Aland Islands, Jan Mayen, French Guiana, Guadeloupe, Martinique, Réunion, Saint Martin (French Part), and Mayotte.

For the sake of clarity, the EEA does not include: Andorra, Monaco, San Marino, Switzerland, Vatican City, Antarctica, Greenland, Faroe Islands, Akrotiri and Dhekelia, Saint Pierre and Miquelon, Saint Barthélemy, Saint Martin (Dutch Part), Svalbard, United Kingdom, Gibraltar, Guernsey, Jersey, Falkland Islands, Isle of Man, Pitcairn, Henderson, Ducie and Oeno Islands, Saint Helena, Ascension and Tristan da Cunha, South Georgia, and the South Sandwich Islands.

European Union (EU)

The following countries, islands and territories: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy,

Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Canary Islands, Ceuta, Melilla, Madeira, Azores, Aland Islands, Mayotte, Martinique, Guadeloupe, French Guiana, Réunion, and Saint-Martin (French Part).

Inter-European PTA Transaction

A PTA Transaction using a PTA Originating Account located in a country or territory listed in Single European Payments Area (SEPA) and using a PTA Receiving Account located in a country or territory listed in Non-Single European Payments Area (Non-SEPA) or a PTA Transaction using a PTA Originating Account located in a country or territory listed in Non-Single European Payments Area (Non–SEPA) and using a PTA Receiving Account located in a country or territory listed in Single European Payments Area (SEPA).

Inter-European Transaction

A Transaction completed using a Card issued in a country or territory listed in Single European Payments Area (SEPA) at a Terminal located in a country or territory listed in Non-Single European Payments Area (Non-SEPA) or Transaction completed using a Card issued in a country or territory listed in Non-Single European Payments Area (Non–SEPA) at a Terminal located in a country or territory listed in Single European Payments Area (SEPA).

Interregional Transaction

In the Europe Region, the term Interregional Transaction includes Inter-European Transactions.

Intracountry PTA Transaction

A PTA Transaction using a PTA Originating Account located in the same country as the location of the PTA Receiving Account.

Intra-EEA Transaction

A Transaction that is not an Intracountry Transaction and that is completed using a Card issued in a country or territory that is part of the EEA at a Terminal located in a country or territory that is part of the EEA and that is acquired by an Acquirer pursuant to a License for a country or territory that is part of the EEA.

Intra–European Transaction

An Intra-Non-SEPA Transaction or an Intra–SEPA Transaction, but not an Inter–European Transaction.

Intra–Non–SEPA PTA Transaction

A PTA Transaction using a PTA Originating Account located in a country or territory listed in Non–Single European Payments Area (Non–SEPA) and using a PTA Receiving Account located in another country or territory listed in Non–Single European Payments Area (Non–SEPA).

Intra–Non–SEPA Transaction

A Transaction completed using a Card issued in a country or territory listed in Non–Single European Payments Area (Non–SEPA) at a Terminal located in a country or territory listed in Non–Single European Payments Area (Non–SEPA).

Intraregional Transaction

This term is replaced by "Intra–European Transaction" in the Europe Region.

Intra-SEPA PTA Transaction

A PTA Transaction using a PTA Originating Account located in a country or territory listed in Single European Payments Area (SEPA) and using a PTA Receiving Account located in another country or territory listed in Single European Payments Area (SEPA).

Intra-SEPA Transaction

A Transaction completed using a Card issued in a country or territory listed in Single European Payments Area (SEPA) at a Terminal located in a country or territory listed in Single European Payments Area (SEPA).

Payment Institution

This term has the meaning set out in Directive (EU) 2015/2366 of 15 November 2015.

Prepaid Card

In the EEA, Gibraltar, and the United Kingdom this term has the meaning set out in EU Regulation 2015/751.

In Serbia, this term has the meaning set out in Serbian Law No. 44/2018.

In Bosnia and Herzegovina, this term has the meaning set out in Law on Interchange Fees for Card-Based Payment Transactions of Republika Srpska.

PSD2 RTS

The 2nd Payment Services Directive (Directive [EU] 2015/2366 of 25 November 2015) Regulatory Technical Standards on Strong Customer Authentication ("SCA").

Remote Electronic Transaction

All types of Card-not-present Transactions (e-commerce Transactions, recurring payment Transactions, installment Transactions, Credential-on-File Transactions, in-app Transactions, and Transactions completed through a Digital Wallet). Mail order and telephone order (MO/TO) Transactions and Transactions completed with anonymous prepaid Cards are excluded from this definition.

SCA Country, SCA Countries

The countries, islands and territories that have adopted legislation requiring Strong Customer Authentication (e.g. legislation transposing the PSD2 RTS, or similar legislation).

These countries are Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Ceuta, Melilla, Azores, Madeira, Aland Islands, Jan Mayen, French Guiana, Guadeloupe, Martinique, Réunion, Saint Martin (French Part), and Mayotte.

UK SFD Regulations

The UK Financial Markets and Insolvency (Settlement Finality) Regulations 1999.

1.6 The License

A License (other than a License to perform Payment Transfer Activity) will cover both issuing and acquiring, unless the applicant or Customer wishes to receive a License for issuing only or acquiring only.

1.6.1 SEPA Licensing Program

An applicant or a Customer with a License for a SEPA country may participate in the SEPA licensing program.

A Customer may participate in the SEPA licensing program as a Principal, Association, or Affiliate. A Principal or Association participating in the SEPA licensing program may Sponsor Affiliates in one or more SEPA countries. An Affiliate may be sponsored by different Sponsors in different countries.

The Customer must undergo additional reviews (for example, risk management and AML compliance) before each additional License is approved. The Customer must meet any applicable legal or regulatory requirements in each country in which it intends to undertake Activities.

Each Sponsoring Customer is assigned a separate ICA for each SEPA country in which it is active, must use that ICA only for its Activity in that country, and must not undertake Activity in that country before the relevant ICA has been implemented.

The Sponsoring Customer is assigned a separate BIN or BIN range for each SEPA country in which it is active, must use that BIN or BIN range only for its Activity in that country, and must not undertake Activity in the country before the relevant BIN or BIN range has been implemented. Different ranges within a BIN may be linked to ICAs assigned for different SEPA countries.

With regard to Intracountry Transactions and/or Intracountry PTA Transactions, a Customer participating in the SEPA licensing program must comply with the applicable intracountry rules and fees.

1.7 Area of Use of the License

In the Europe Region, the Rule on this subject is modified as follows.

In the EEA, the License covers the entire EEA as the Area of Use.

A separate ICA is required for ATM acquiring in each EEA country. A separate ICA and BIN or BIN range is required for issuance in each EEA country.

Different ranges within a BIN assigned to an Issuer may be linked to ICAs assigned to that same Issuer for different countries. A Customer is not required to have a physical establishment in the Area of Use.

A single ICA may be used for Merchant acquiring in the United Kingdom, Gibraltar, and one or more EEA countries.

1.7.1 Extending the Area of Use

For Customers that have a License for the EEA, Gibraltar, or the United Kingdom, the Rule on this subject is modified as follows.

A Principal or Association Customer may apply for an extension of its Area of Use to Sponsor an entity that is located in a country different from the country in which the Principal or Association Customer is incorporated or otherwise constituted.

The entity proposed to be Sponsored:

a. Must be authorized to engage in Activity under the laws or government regulations of an EEA country, Gibraltar, or the United Kingdom;

b. Must limit its Activity to the Area of Use mentioned in its License.

1.7.2 Extension of Area of Use Programs

A Customer with a License for the EEA is not required to apply for an extension of Area of Use in order to undertake Activity in an additional country within the EEA.

1.7.3 Central Acquiring

In the Europe Region, Rule 1.7.3 replaces Rule 1.7.2, paragraph 6.

A Customer that complies with this Rule 1.7.3, may acquire Transactions from a Europe Region Merchant located outside of its Area of Use, with the exception of Merchants located in the Russian Federation, where central acquiring is not permitted.

1.7.3.1 Central Acquiring Registration

A Customer must have completed the central acquiring registration process before it centrally acquires.

The central acquiring registration letter specifies the countries in which a Customer may centrally acquire intra–European and inter–European Transactions from a Merchant.

In order to be registered for central acquiring, the Customer must meet the central Acquirer criteria set forth in Rule 1.7.3.2.

1.7.3.2 Central Acquirer Service Requirements

The Customer must authorize, clear and settle centrally acquired Transactions in a manner that does not disadvantage the Cardholder, the Merchant, or the Issuer involved in the Transaction in comparison with non-centrally acquired Transactions.

1.7.3.3 Intracountry Rules

A central Acquirer must comply with the intracountry rules of each country in which Transactions are centrally acquired.

1.7.3.4 Centrally Acquired Merchants

An Acquirer may centrally acquire Transactions from **any Merchant** located in any one of the following **Western or Central European Areas of Use**: EEA, Andorra, United Kingdom, Gibraltar, Guernsey, Jersey, Isle of Man, Monaco, San Marino, Switzerland, Turkey, Vatican City.

In **all other Europe Region countries**, excluding the Russian Federation, an Acquirer may only centrally acquire Transactions of a Merchant that operates in more than two Europe Region countries. However, an Acquirer may centrally acquire e-commerce Transactions from an e-commerce Merchant operating in only one Europe Region country pursuant to its central acquiring authorization.

1.7.3.5 Registration Procedure

To register to centrally acquire Merchants located in the **Western and Central European Areas of Use** listed in Rule 1.7.3.4, the Customer must submit to the Corporation a single application form covering all such Western and Central European Areas of Use.

The central acquiring registration letter will cover all such Western and Central European Areas of Use.

To register to centrally acquire Merchants located in other countries, the Customer must submit to the Corporation an application form for each Merchant and country where the Customer wishes to centrally acquire Transactions.

1.7.3.6 Extension of Registration

In the **Western and Central European Areas of Use** listed in Rule 1.7.3.4, a central Acquirer is not required to comply with any formal procedures in order to extend its central acquiring Activities in Western and Central Europe.

In **all other Europe Region countries**, excluding the Russian Federation, a Customer that wishes to extend its central acquiring Activities to a new Merchant or country must follow the registration procedure set forth in Rule 1.7.3.5 above.

1.7.3.7 Interchange Fee Requirements

If a central Acquirer acquires an Intracountry Transaction, the following principles apply to the interchange fee:

1. The central Acquirer may agree upon bilateral interchange fees with the Issuer; and
2. Unless a bilateral agreement applicable to an Intracountry Transaction has been established between two Customers, then the interchange fees applicable to an Intracountry Transaction as set forth in the *Interchange Manual—Europe Region*, will apply.

If a central Acquirer acquires a Non-Intracountry Transaction, the following principles apply to the interchange fee:

1. The central Acquirer may agree upon bilateral interchange fees with the Issuer; and
2. Unless a bilateral agreement applicable to a Non-Intracountry Transaction has been established between two Customers, the interchange fees applicable to a Non-Intracountry Transaction as set forth in the *Interchange Manual - Europe Region*, will apply.

1.7.3.8 Settlement of Disputes

Any disputes relating to central acquiring will be resolved by the Corporation in accordance with the Standards.

1.7.3.9 Customer Noncompliance

The following are examples of violations of the central acquiring rules for which noncompliance assessments may be applied:

1. Engaging in central acquiring without first registering,
2. Engaging in central acquiring in non-notified countries or of non-notified Merchants (not applicable for Western and Central European countries).
3. Failure to comply with intracountry rules (including application of incorrect interchange fees) resulting in financial loss to another party.
4. Incorrect data in Transaction messages (including incorrect country code) resulting in financial loss to another party.

1.13 Termination of License

1.13.2 Termination by the Corporation

Paragraph 4 of the Rule on this subject does not apply in the Europe Region.

2.1 Standards

2.1.8 Rules Applicable to Intracountry Transactions

The Corporation may establish Rules for Intracountry Transactions and for Intracountry PTA Transactions.

The Corporation will inform Customers of all Rules it establishes.

NOTE: This Rule 2.1.8 does not apply to the establishment of intracountry interchange and service fees. Refer to Rule 8.4, "Establishment of Intracountry Interchange and Service Fees" for more information.

2.1.8.1 Order of Precedence

For any Intracountry Transaction in a SEPA country, the intracountry Rules established by the Corporation apply, or if none, the Rules applicable to Intra-SEPA Transactions apply, or if none, the Rules applicable to Inter-European Transactions apply, or if none, the interregional Rules apply.

For any Intracountry Transaction in a Non–SEPA country, the intracountry Rules established by the Corporation apply, or if none, the Rules applicable to Intra–Non–SEPA Transactions apply, or if none, the Rules applicable to Inter–European Transactions apply, or if none, the interregional Rules apply.

For any Intracountry PTA Transaction in a SEPA country, the intracountry Rules established by the Corporation apply, or if none, the Rules applicable to Intra-SEPA PTA Transactions apply, or if none, the Rules applicable to Inter-European PTA Transactions apply, or if none, the interregional Rules apply.

For any Intracountry PTA Transaction in a Non–SEPA country, the intracountry Rules established by the Corporation apply, or if none, the Rules applicable to Intra–Non–SEPA PTA Transactions apply, or if none, the Rules applicable to Inter–European PTA Transactions apply, or if none, the interregional Rules apply.

2.4 Choice of Laws

In the Europe Region, the Rule on this subject is replaced in its entirety by the following:

Licenses are governed by and construed according to the applicable law mentioned in the particular License, without reference to conflict-of-laws or similar provisions that would mandate or permit application of the substantive law of any other jurisdiction.

The courts mentioned in the particular License have exclusive jurisdiction for the resolution of any dispute relating to rights and obligations deriving from Licenses.

Licenses concluded after 31 January 2020 specify English law and courts or Belgian law and courts, as chosen by the Customer.

The Standards are governed by and construed according to Belgian law, without reference to conflict-of-laws or similar provisions that would mandate or permit the application of substantive law of any other jurisdiction. Belgian courts have exclusive jurisdiction for the resolution of any dispute relating to the Standards between two Customers holding Licenses for countries in the Europe Region.

3.1 Obligation to Issue Mastercard Cards—EEA, Gibraltar, and United Kingdom Only

The Rule on this subject does not apply in the EEA, Gibraltar, or the United Kingdom.

3.3 Transaction Requirements—SEPA Only

Paragraph 5 of the Rule on this subject does not apply to Cross-border Transactions that are Intra-SEPA Transactions.

3.6 Non-discrimination—ATM and Bank Branch Terminal Transactions

In the Europe Region, the Rule on this subject is modified as follows.

An Acquirer must not discriminate against any Card, with regard to processing Transactions, including Cards issued by other Customers in the same country.

An Issuer must not discriminate against any ATM Terminal or Bank Branch Terminal with regard to processing and authorizing Transactions, including ATM Terminals and Bank Branch Terminals owned by other Customers within the same country.

These non-discrimination Rules also apply with regard to balance inquiry and PIN change/unblock functionality provided at ATM Terminals, according to the Card category (e.g., debit, credit).

3.13 Privacy and Data Protection

3.13.8 Regional Variances and Additions

A Customer that is subject to Applicable Data Protection Law in the Europe Region must comply with both Rule 3.13 as set forth in Chapter 3, "Customers Obligations", and this Rule 3.13.8, which applies to Processing of Personal Data subject to EU Data Protection Law. This Rule 3.13.8 does not apply to switching services relating to Intra-EEA Transactions, Transactions between an EEA country, Gibraltar, or the United Kingdom, or Intracountry Transactions within an EEA country, Gibraltar, or the United Kingdom, which are governed by the *Mastercard Switch Rules*.

As used in this Rule, the following terms have the meanings as described below.

Controller

The entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

Disclosure Request

Means any request by a Government Agency for access to, or disclosure of, Personal Data for law enforcement, national security regulatory reporting or other purposes.

EU Data Protection Law

The EU General Data Protection Regulation 2016/679 (GDPR) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC implementing and any legislation or regulation or made pursuant to them in any country in the EEA; the UK GDPR and Data Protection Act 2019; the Monaco Data Protection Act; the Swiss Federal Data Protection Act ("FADP") ; the UK Data Protection Act; and the Data Protection Acts of the EEA countries; and any legislation and/or regulation which amends, replaces, re-enacts or consolidates any of them.

Government Agency

Any competent public or quasi-public authority (including without limitation regulators, local government authorities, law enforcement authorities and national security agencies) of any jurisdiction that may request disclosure of Personal Data Processed in connection with Activity and Digital Activity.

Mastercard Binding Corporate Rules (Mastercard BCRs)

The Mastercard Binding Corporate Rules as approved by the EEA data protection authorities, available on the Corporation's public facing website.

Standard Contractual Clauses or SCCs

With respect to Personal Data to which the GDPR applies, the standard contractual clauses for the transfer of Personal Data to Third Countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, and not including any clauses marked as optional ("EU Standard Contractual Clauses" or "EU SCCs").

With respect to Personal Data to which the FADP applies, the EU SCCs, provided that any references in the clauses to the GDPR shall refer to the FADP.

With respect to Personal Data to which the UK GDPR applies, the International Data Transfer Addendum to the EU SCCs ("UK Addendum"), issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but, as permitted by clause 17 of the UK Addendum, Customer and the Corporation agree to change the format of the information set out in Part 1 of the UK Addendum so that:

- the details of the Corporation and Customer in table 1 of the UK Addendum shall be as set out in Annex 1 of Section 3.13.8.12 (with no requirement for signature);
- for the purposes of table 2 of the UK Addendum the first option is selected and the "Approved EU SCCs" are those incorporated as per the paragraph above; and
- the appendix information listed in table 3 of the UK Addendum is set out in Annex 1 and Annex 2 of Section 3.13.8.12.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or other unauthorized Processing of Personal Data transmitted, stored, or otherwise Processed.

Processor

The entity which Processes Personal Data on behalf of a Controller.

Sensitive Data

Any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any future revision of EU Data Protection Law.

Sub-Processor

The entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

Third Country

A country where the laws applicable to Personal Data do not offer the same level of protection for such Personal Data as the laws applicable in the country where the Customer's Data Subject is located.

UK Data Protection Law

The Data Protection Act 2018; the GDPR, as amended by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 ('UK GDPR') as relevant; and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) as transposed into UK national law.

3.13.8.1 Processing of Personal Data for Purposes of Activity and Digital Activity

In the Europe Region, Rule 3.13.1 is modified to include the following.

A Customer is a Controller with regard to the Processing of Personal Data for the purposes of carrying out the Customer's Activities and Digital Activities, and the Corporation acts as a Processor for these purposes.

Each Customer acknowledges that the Corporation may Process, as a Controller, Personal Data for the purposes of accounting, auditing and billing; fraud, financial crime and risk management; defense against claims, litigation and other liabilities; arbitration and other decisions relating to dispute resolution; product development and improvement; internal research, reporting and analysis; anonymization of data to develop data analytics products; and compliance with legal obligations. The Corporation represents and warrants that the Corporation will Process Personal Data for these purposes in compliance with EU Data Protection Law and the

Standards and in line with the description of the Processing activities set forth in the Mastercard BCRs.

To the extent that it acts as a Processor, the Corporation will: (1) cooperate with Customers in their role as Controllers to fulfill their data protection compliance obligations in accordance with EU Data Protection Law; (2) only undertake Processing of Personal Data in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in the Standards, the Mastercard BCRs, or as otherwise agreed in writing; and (3) comply with obligations equivalent to those imposed on the Customers as Controllers by the applicable provisions of EU Data Protection Law, including those applicable to Processors and data transfers.

The Corporation will notify the Customer when local laws prevent the Corporation (1) from complying with the Customer's instructions (except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), and (2) from fulfilling its obligations under the Standards or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by the Standards or the Mastercard BCRs.

3.13.8.2 Mastercard BCRs

The Corporation will abide by the Mastercard BCRs when the Processing of Personal Data is or was subject to EU Data Protection Law.

3.13.8.3 Data Subject Notice and Consent

In the Europe Region, Rule 3.13.2 is modified to include the following.

A Customer must ensure that the Processing of Personal Data for the purposes provided in Rule 3.13.1, relies on a valid legal ground under EU Data Protection Law, including obtaining Data Subjects' proper consent where required or appropriate under EU Data Protection Law.

A Customer must ensure that Data Subjects receive appropriate notice, in a timely manner: (1) with at the minimum all of the elements required under EU Data Protection Law, (2) about the existence of Processors located outside of the EEA or the relevant country where relevant; and (3) where required or appropriate, about the existence of the Mastercard BCRs, including about Data Subjects' right to enforce the Mastercard BCRs as third-party beneficiaries (by referring to the public version of the Mastercard BCRs).

3.13.8.4 Data Subject Rights

In the Europe Region, Rule 3.13.3 is modified to include the following.

A Customer must develop and implement appropriate procedures for handling Data Subjects' requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing of Personal Data, (f) objection, and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them.

To the extent that the Corporation acts as a Processor, the Corporation will assist the Customer in complying with its obligation to respond to such requests, including by providing access to Personal Data maintained by the Corporation.

3.13.8.5 Accountability

Taking into account the nature, scope, context, and purposes of Processing of Personal Data, as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, the Corporation and the Customers must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that Processing of Personal Data is performed in accordance with the Standards and EU Data Protection Law, including, as applicable, by appointing a data protection officer, maintaining records of Processing of Personal Data, complying with the principles of data protection by design and by default, performing data protection impact assessments, appropriate documentation on international transfers of Personal Data and conducting prior consultations with supervisory authorities. The Corporation will cooperate with and assist the Customers in fulfilling their own obligations under EU Data Protection Law.

3.13.8.6 International Data Transfers

Each Customer authorizes the Corporation to transfer the Personal Data Processed subject to EU Data Protection Law outside of the Europe Region, and in particular into the United States Region and India, in accordance with the Mastercard BCRs or with any other lawful data transfer mechanism that provides an adequate level of protection under EU Data Protection Law.

To the extent that the Corporation makes any transfer of Personal Data Processed in connection with the Activity or Digital Activity to an entity in a Third Country outside the scope of the Mastercard BCRs (for which another lawful data transfer mechanism is required to provide an adequate level of protection under EU Data Protection Law or UK Data Protection Law), the Corporation and the Customer agree to enter into and comply with the obligations set out in the SCCs, which are hereby incorporated by reference, as though such obligations were set out in full in these Standards, and with the Customer's and the Corporation's signature and dating of the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound by these Standards being deemed to be the signature and dating of the SCCs.

The EU SCCs are completed as follows: the Corporation and Customer conclude module four of the EU SCCs (processor-to-controller) of the EU SCCs.

- The "data exporter" is the Corporation; the "data importer" is the Customer;
- Clause 16 (Governing law): the clauses shall be governed by the laws of Belgium;
- The information as required by Annex I of the SCCs is as set out in Annex 1 of this section

If the Corporation's compliance with EU Data Protection Law or UK Data Protection Law applicable to international data transfers is affected by circumstances outside of the Corporation's control, including if a legal instrument for international data transfers is invalidated, amended, or replaced, then Customer and the Corporation will work together in good faith to reasonably resolve such non-compliance.

In the event the Corporation is compelled to comply with a Disclosure Request and such disclosure causes Customer to breach EU Data Protection Law or UK Data Protection Law, the Customer represents and warrants that it will not hold the Corporation liable for such disclosure. The Customer further agrees that, to the greatest extent authorized by applicable law, it will not revoke or amend its instruction to Process Personal Data unless strictly required by EU Data Protection Law. Any amendments to the Customer's instructions to Process Personal Data, such as where necessary to ensure the continued compliance with EU Data Protection Law, must be agreed by both the Corporation and Customer in writing prior to taking effect.

3.13.8.7 Sub-Processing

In the Europe Region, Rule 3.13.6 is modified to include the following.

To the extent that the Corporation acts as a Processor, the Customer, gives a general authorization to the Corporation to Process and sub-Process Personal Data to internal and external Sub-Processors in the context of the Customer's Activities and Digital Activities under the conditions set forth below and when sub-Processing the Processing of Personal Data in the context of the Customer's Activities and Digital Activities, the Corporation:

- Binds its internal Sub-Processors to respect Mastercard BCRs and to comply with the Customer's instructions.
- Requires its external Sub-Processors, via a written agreement, to comply with the requirements of EU Data Protection Law applicable to Processors and data transfers, with the Customer's' instructions, and with the same obligations as are imposed on the Corporation by the Standards and the Mastercard BCRs, including sub-Processing and audit requirements set forth in Mastercard BCRs
- Remains liable to the Customer for the performance of its Sub-Processors' obligations.
- Commits to provide a list of Sub-Processors to the Customer upon request.
- Will inform Customer of any addition or replacement of a Sub-Processor in a timely fashion so as to give Customer an opportunity to object to the change before the Personal Data is communicated to the new Sub-Processor.

The Corporation requires its external Sub-Processors, via a written agreement, to comply with the requirements of EU Data Protection Law applicable to Processors and data transfers, with the Customers' instructions, and with the same obligations as are imposed on the Corporation by the Standards and the Mastercard BCRs. The Corporation acting as a Processor is authorized by the Customer, acting as a Controller, to enter into the 2010 Controller to Processor Standard Contractual Clauses with non-EEA-based Sub-Processors on behalf of Customers. The Corporation will remain liable to the Customer for the performance of its Sub-Processors' obligations.

3.13.8.8 Government Requests for Personal Data

Where the Corporation is requested to disclose Personal Data to a Government Agency that the Corporation is Processing, the Corporation will only comply with such request in accordance with the Mastercard BCRs and EU Data Protection Law. Where the Corporation is acting as a

Processor, the Corporation will refer the Government Agency to the Customer, unless the Corporation is prohibited from doing so.

3.13.8.9 Security and Data Protection Audit

In accordance with the Standards and EU Data Protection Law, the Corporation and each Customer must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including during the transmission of the Personal Data.

In assessing the appropriate level of security, the Corporation and the Customer must take into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of Processing, of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

The Corporation and each Customer must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and as applicable Processes Personal Data in accordance with the Customer's instructions.

Upon prior written request by the Customer, to the extent that the Corporation acts as a Processor and subject to the strictest confidentiality obligations, the Corporation will, within reasonable time, provide a Customer with: (a) a summary of the audit reports demonstrating the Corporation's compliance with EU Data Protection Law and Mastercard BCRs, after redacting any confidential or commercially sensitive information; and (b) a confirmation that the audit has not revealed any material vulnerability in the Corporation's systems, or to the extent that any such vulnerability was detected that the Corporation has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with EU Data Protection Law and the Mastercard BCRs, or reveal some material issues, subject to the strictest confidentiality obligations, the Corporation will allow the Customer to request an audit of the Corporation's data protection compliance program by external independent auditors, which are jointly selected by the Corporation and the Customer. The external independent auditor cannot be a competitor of the Corporation, and the Corporation and the Customer will mutually agree upon the scope, timing, cost and duration of the audit. The Corporation will make available to the Customer the result of the audit of its data protection compliance program.

3.13.8.10 Personal Data Breaches

Where the Corporation acts as a Processor, and where required under EU Data Protection Law, the Corporation will inform the Customer, without undue delay, and no later than 48 hours after having become aware of it, of a Personal Data Breach.

The Corporation will assist the Customer in complying with its own obligations to notify a Personal Data Breach. The Corporation and each Customer must document all Personal Data

Breaches, including the facts relating to the Personal Data Breach, its effects, and the remedial action taken.

3.13.8.11 Liability for EU Data Protection Law Violations

Where the Customer or the Corporation acts as a Controller, it is responsible for the damage caused by the Processing of Personal Data which infringes the Data Protection sections in the Standards and EU Data Protection Law. To the extent that the Corporation acts as a Processor, it will be liable for the damage caused by Processing of Personal Data only where it has not complied with obligations of EU Data Protection Law specifically directed to Processors or where it has acted outside or contrary to lawful instructions of the Customer. The Corporation will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where one or more Customers and/or the Corporation are involved in the same Processing of Personal Data and where they are responsible for any damage caused by Processing of Personal Data, each may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If the Corporation paid full compensation for the damage suffered, it is entitled to claim back from the Customer(s) involved in the same Processing of Personal Data that part of the compensation corresponding to their part of responsibility for the damage.

3.13.8.12 Annexes for Processing of Personal Data

Annex 1 to Section 3.13.8: Processing of Personal Data

A. List of Parties

1. Data exporter: Corporation
   - Name and address of the Corporation as well as the name, position, and contact details for the Corporation's contact person: as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other documents by which Customer is bound.
   - Activities relevant to the data transferred: Activity and Digital Activity
   - Signature and date: as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or another documents by which Customer is bound.
   - Role: As set out in Rule 3.13.8.1 or as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other documents by which Customer is bound.
2. Data importer: Customer
   - Name and Address of Customer as well as the name, position, and contact details for Customer's contact person: as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound
   - Activities relevant to the data transferred: Participating in, or benefiting from, the Activity or Digital Activity.

- Signature and date: as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, or license agreement by which Customer is bound by those Standards
- Role: As set out in Rule 3.13.8.1 of those Standards or as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other documents by which Customer is bound.

B. Description of the Transfer

Data Subjects

As stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Categories of data

Confidential Transaction Data, including PAN data, date, time and amount of Transaction or as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Sensitive Data transferred

The Customer and the Corporation do not Process any Sensitive Data in the context of the Activity and the Digital Activity unless as stipulated otherwise in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Frequency of the transfer

Continuous.

Nature of the Processing

Collection, storage, analysis, disclosure by transfer or otherwise making available.

Purposes of the transfer(s)

The transfer is made for the purposes set forth in Rule 3.13.8.1 or as stipulated in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Period for which the Personal data will be retained

Personal Data will be retained only for as long as necessary to provide the services covered under the Activity and the Digital Activity.

C. Competent Supervisory Authority

The Belgian Data Protection Authority.

Annex 2 to Section 3.13.8: Technical and Organizational Measures to Ensure the Security of Data

The Customer and the Corporation will, as a minimum, implement the following types of security measures:

Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, including:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (e.g., ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Having door locking (e.g., electric door openers);
- Having security staff or janitors;
- Using Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons, including:

- User identification and authentication procedures;
- ID/password security procedures (e.g., special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts; and
- Creation of one master record per user, user master data procedures, per data processing environment.

Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (e.g., profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;

- Change procedure; and
- Deletion procedure.

Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, including:

- Tunneling
- Logging; and
- Transport security.

Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including:

- Logging and reporting systems; and
- Audit trails and documentation.

Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the instructions of the Controller, including:

- Unambiguous wording for the Controller's instructions;
- Formal commissioning (request form); and
- Criteria for selecting the Processor.

Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical), including:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply);
- Remote storage;
- Anti-virus/firewall systems; and
- Disaster recovery plan.

Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately, including:

- Separation of databases;
- Access and use restrictions on a need-to-know basis
- Segregation of functions (e.g., production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

Annex 3 to Section 3.13.8: Sub-Processing of Personal Data

List of Sub-Processors

As listed in https://techdocs.mastercard.com/bundle/m_GDPR/page/vcd1642413792117.html or in the relevant License Agreement, Digital Activity Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

3.16 Issuer Reporting Requirement—EEA, Andorra, Serbia, Bosnia and Herzegovina, Gibraltar, and United Kingdom

With regard to Intra-EEA Transactions (as defined in the Europe Region chapter), Transactions between the EEA and Andorra, Gibraltar or the United Kingdom, and Intracountry Transactions in EEA countries, Andorra, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom, each Customer must keep an account, on a calendar year basis, of the total amount of scheme-related fees that each has paid, directly or indirectly, to the Corporation as an Issuer, and of the total amount, if any, that each has received as an Issuer from the Corporation. If the amount received exceeds the amount paid, the Customer must contact its relationship manager prior to 1 April of the following year to resolve the net compensation event.

3.17 BINs

In the Europe Region, the Rule on this subject is modified as follows.

BINs assigned to the Corporation by ISO must be used only to issue Mastercard, Maestro or Cirrus Cards and to carry out Mastercard, Maestro or Cirrus Transactions, unless otherwise agreed in writing.

4.1 Right to Use the Marks

4.1.1 Protection and Registration of the Marks

In the Europe Region, the Rule on this subject is modified as follows.

Mastercard Europe SA is the exclusive owner of the Eurocard and eurocheque marks. A Customer must not, either by act or omission, do anything inconsistent with the exclusive ownership of the Eurocard or eurocheque marks, or do anything that may harm the Eurocard or eurocheque marks.

A Customer must take such measures as the Corporation or other owner of a Mark may require to assist in any actions by the Corporation or other owner to register, perfect, maintain, or protect the Corporation's or other owner's rights to the Mark. The Customer may be required by the Corporation or other owner to litigate in the Customer's own name, on behalf of the owner of the Mark, if the owner is legally prevented from litigating in its own name. All activities

relating to such assistance will be decided upon and be under the control of the Corporation or the other owner of the Mark. The owner will pay the Customer's reasonable out-of-pocket expenses related to these activities.

4.4 Signage System

In Germany, the Rule on this subject is modified as follows.

When displayed, the ec Mark must be placed between the Mastercard Mark and the Maestro Mark.

4.4.2 ATM Terminal Signage

When displayed on an ATM located in Germany, the ec Mark must be placed between the Mastercard Mark and the Maestro Mark.

4.8 Use of Marks on Maestro and Cirrus Cards

In the Europe Region, the Rule on this subject is modified as follows.

1. The Maestro Mark may co-reside on a Mastercard Card in the context of a Corporation-approved multi-Account Card Program.
2. A Customer must not use the trademark or trade name of a competing international payment scheme on Maestro Cards or Cirrus Cards, unless it has received written permission from the Corporation to do so. This Rule does not apply in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, or the United Kingdom.
3. In the EEA, Gibraltar, and the United Kingdom the Maestro Brand Mark may be placed on any type of card, including Credit Cards and Commercial Cards.
4. In the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom the Maestro Mark may co-reside on a Card with other payment scheme marks. Each payment scheme is identified by its logo or mark displayed on Cards and at the POI and by its distinct AID in the chip of the Card. When another payment scheme co-resides on a Maestro Card, the Issuer must clearly inform the Cardholder how to use the Maestro Payment Application.

4.9 Use of Marks on Mastercard Cards

The Rule on this subject is modified as follows.

In the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom, the Marks may co-reside on Mastercard Cards with other payment scheme marks. Each payment scheme is identified by its logo or mark displayed on Cards and at the POI and by its distinct AID in the chip of the Card. When another payment scheme co-resides on a Mastercard Card, the Issuer must clearly inform the Cardholder how to use the Mastercard Payment Application.

5.1 The Merchant and ATM Owner Agreements

5.1.2 Required Merchant Agreement Terms

In the Europe Region, the Rule on this subject is modified as follows.

Each Merchant Agreement with a Merchant located in the EEA, Gibraltar, or the United Kingdom must contain a term requiring the Merchant to respond to Cardholder disputes and handle chargebacks in accordance with the *Chargeback Guide*.

5.4 Acquirer Obligations to Merchants

5.4.3 Provide Information

An Acquirer in the EEA must inform a Merchant of any changes to the terms of the Merchant Agreement that result from changes made by the Corporation to the Standards.

This information must be provided with at least 2 months advance notice whenever possible.

An Acquirer may provide a Merchant located in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, or the United Kingdom with information enabling the Merchant to identify the category (business/commercial, debit, credit, or prepaid) of each Card or Payment Application issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, or the United Kingdom.

5.5 Merchant Location

Merchant Location for Card-Not-Present Transactions

The following Rule modification applies with regard to Transactions on consumer cards issued outside of the EEA completed at a Merchant located in the EEA.

The Merchant location for Card-not-present Transactions is the address of the fixed place of business through which the Merchant conducts its business including the supporting operations through which the Transaction is completed, regardless of website or server locations.

If the Merchant does not have a fixed place of business, the Merchant location is the address for which the Merchant holds a valid business license and through which the Transaction is completed.

A Merchant and its Acquirer may, at their sole option, after consultation with, but without being directed by, the Corporation, determine that a Merchant is located in an EEA country as follows:

(a) travel-related Merchants, a location within the country where the first leg of the journey begins;

(b) lodging Merchants, a location within the country where accommodation is provided;

(c) car rental, taxi or ride service Merchants, a location within the country where the Cardholder rents the vehicle; and

(d) travel agencies, a location within the country of the travel agent.

5.5.1 Disclosure of Merchant Name and Location

The following additional Rule applies to Intra-EEA Transactions and to Intracountry Transactions in the EEA.

An Acquirer must ensure that a Merchant always uses the same name in authentication messages for Remote Electronic Transactions. The Merchant name in the authentication must uniquely identify the Merchant in all countries where it operates and for all its activities (e.g., Merchant.com) or per its activities (such as, MerchantBooks.com, MerchantMusic.com) or per its countries (such as, Merchant.fr, Merchant.co.uk).

It is recommended that the Merchant name is the same in authentication and authorization.

An Acquirer must ensure that the name used by the Merchant actually belongs to the Merchant and is registered for use in the Identity Check Program. An Acquirer must ensure that the Merchant name used during authentication and registered in ISSM is not used by another Merchant.

5.6 Submerchant Location

The Rule modification set out in Rule 5.5 of this Chapter also applies with regard to Card-not-present Transactions on consumer cards issued outside of the EEA completed at a Submerchant located in the EEA.

5.6.1 Disclosure of Submerchant Name and Location

The following additional Rule applies to Intra-EEA Transactions and to Intracountry Transactions in the EEA.

An Acquirer must ensure that a Submerchant always uses the same name in authentication messages for Remote Electronic Transactions. The Submerchant name in the authentication message must uniquely identify the Submerchant in all countries where it operates and for all its activities (such as, Merchant.com) or per its activities (such as, MerchantBooks.com, MerchantMusic.com) or per its countries (such as, Merchant.fr, Merchant.co.uk).

It is recommended that the Submerchant name is the same in authentication and authorization.

The authentication must include the name of the Payment Facilitator, in full or in abbreviated form, followed by "*" and the Submerchant name.

An Acquirer must ensure that the name used by the Submerchant actually belongs to the Submerchant and is registered for use in the Identity Check Program.

5.8 Transaction Message Data

In the EEA, Gibraltar, and the United Kingdom the Rule on this subject is modified as follows.

A Customer must refer to the specifications manuals of the registered switch of its choice for technical requirements relating to Transaction data.

5.8.2 Card Acceptor Address Information

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

The address of a Terminal or website must be indicated in the field specified by the registered switch of the Customer's choice.

5.8.3 Submerchant Name Information

In the EEA, Gibraltar, and the United Kingdom the Rule on this subject is modified as follows.

The name and location of a Merchant, Payment Facilitator and Sub-merchant, as appropriate, must be indicated in the field specified by the registered switch of the Customer's choice.

5.8.4 ATM Terminal Information

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

The ATM owner name, ATM location, and unique ATM Terminal identification must be indicated in the fields specified by the registered switch of the Customer's choice. Unique numbers identifying the Acquirer and any Service Provider must be assigned by the registered switch of the Customer's choice.

5.8.5 Transactions at Terminals with No Fixed Location

Refer to Rule 5.5 of this Chapter for a Rule modification applicable with regard to Card-not-present Transactions on consumer cards issued outside of the EEA completed at a Merchant in the EEA that has no fixed place of business.

5.11 Merchant Obligations for Acceptance

5.11.1 Honor All Cards

In the Europe Region, the Rule on this subject is modified as follows.

EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom

The following Rules apply with respect to acceptance by Merchants in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom, of Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.

1. A Merchant that accepts Mastercard Credit Cards must accept all Mastercard Credit Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.

2. A Merchant that accepts Mastercard Debit Cards, including Debit Mastercard Cards, must accept all Mastercard Debit Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.
3. A Merchant that accepts Mastercard Prepaid Cards must accept all Mastercard Prepaid Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.
4. A Merchant that accepts Maestro Credit Cards must accept all Maestro Credit Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.
5. A Merchant that accepts Maestro Debit Cards must accept all Maestro Debit Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.
6. A Merchant that accepts Maestro Prepaid Cards must accept all Maestro Prepaid Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.
7. A Merchant is not required to accept Maestro Cards as a condition of accepting Mastercard Cards, and vice versa.
8. A Merchant is not required to accept Commercial Cards issued in the EEA, Bosnia and Herzegovina, Gibraltar, and the United Kingdom or Business Cards issued in Serbia.
9. A Merchant must not refuse to accept any Card on the basis of the identity of the Issuer or the Cardholder.

NOTE: Rule 5.11.1 in Chapter 5 applies with respect to acceptance by Merchants in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom of Cards issued in countries and territories that are not part of the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.

Debit Mastercard—Non-EEA Countries, excluding Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom

The Rule on this subject, as it applies to Debit Mastercard Card acceptance in a non-EEA country (excluding Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom), is modified as follows.

A Merchant in a Debit Mastercard Country that chooses to accept only Debit Mastercard Cards issued in the Europe Region must honor all valid Debit Mastercard Cards issued in the Europe Region without discrimination, when properly presented for payment.

5.11.2 Merchant Acceptance of Mastercard Cards

A Merchant that accepts Mastercard Cards must accept all types of Mastercard Cards (for example, Mastercard consumer Cards, Mastercard Corporate Card®, World Mastercard® Cards, and Debit Mastercard Cards).

The above Rule does not apply with respect to acceptance by Merchants in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom of Cards issued in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, or the United Kingdom.

5.11.2.1 Acceptance in a Debit Mastercard Country

As an exception to Rule 5.11.2 above, a Merchant in a Debit Mastercard Country is permitted to choose to accept only Debit Mastercard Cards issued in the Europe Region or both Debit

Mastercard Cards and other Mastercard Cards issued in the Europe Region. An Acquirer must inform existing and prospective merchants that they have this right.

A Merchant may choose to stop accepting other Mastercard Cards issued in the Europe Region by providing no less than 30 days advance written notice to its Acquirer. The Acquirer must identify to the Corporation any Merchant in a Debit Mastercard Country that chooses to accept Debit Mastercard Cards but not other Mastercard Cards issued in the Europe Region, and inform the Corporation of the reason for the Merchant's decision. Merchants may request signage for the purpose of indicating their acceptance of Debit Mastercard Cards at Debit Mastercard—Non-EEA Countries Only, excluding Serbia, Gibraltar, and the United Kingdomwww.mastercardweacceptdebit.com.

An Acquirer must provide a complete list of accurate and current BINs obtained through the Corporation that apply to Debit Mastercard Cards to its Merchants and ensure that its Merchants use the updated BIN information within six calendar days of such file being made available by the Corporation.

5.11.5 Discounts or Other Benefits at the Point of Interaction

A discount or other benefit may be applied at a POI location in the Europe Region upon simple presentation of a particular Mastercard Card or Maestro Card for payment.

The promotion at the POI of a discount or other benefit that may be accessed by any particular Card is prohibited. The preceding Rule on promotion does not apply in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom.

5.12 Prohibited Practices

5.12.1 Discrimination

EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom

In the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

A Merchant must not be prevented from expressing a preference for the use of the Mastercard or Maestro Payment Application.

Neither a Customer nor a Digital Activity Customer, Merchant, Payment Facilitator or other Service Provider may, directly or indirectly, prevent the use of Mastercard, Maestro, or Cirrus as a brand for Intracountry Transactions in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom, for Transactions between Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom and an EEA country, or for Intra-EEA Transactions.

Chip Environment

By way of example but not limitation, the following requirements apply in the **chip** environment:

1. A single certification must be valid for both intracountry and intra-EU use of a Mastercard, Maestro, or Cirrus Payment Application at the Terminal.
2. The prevalence of any particular chip-based payment application at the Terminal or Acquirer host system level must not be mandated.
3. If a Mastercard, Maestro, or Cirrus Payment Application is supported by both the Card and the Terminal, its use must not be blocked or impaired by technical or other means, such as software in the Terminal.
4. When supported, the Mastercard or Maestro Payment Application must be shown clearly. If the Merchant has pre-selected a payment application, the fact of pre-selection must be shown clearly on the Terminal, along with the means for the Cardholder to override the pre-selection, until the Cardholder has chosen to either accept or override the pre-selection. The means to override the pre-selection must always be offered via the Terminal, which must face the Cardholder, and not only verbally by the Merchant. The difference between overriding the pre-selection and cancelling the Transaction must be shown clearly to the Cardholder via the Terminal, for example a "change application" key separate from the "cancel" key.
5. If a Mastercard, Maestro, or Cirrus Payment Application is supported by both the Card and the Terminal, the Cardholder must be given the opportunity to complete the Transaction with such Payment Application, unless the Terminal has no screen and/or PIN pad. In that case, the priority order defined in the Terminal, if any, may be used.
6. Debit Mastercard—Non-EEA Countries Only, excluding Serbia,The payment application selected by the Cardholder on the Terminal must not be overridden by technical or other means, such as software in the Terminal. The Cardholder's chosen payment application must not be converted to a different payment application from that chosen by the Cardholder.

Electronic Commerce Environment

By way of example but not limitation, the following requirements apply for Transactions completed in an **electronic commerce** environment.

1. The Merchant must clearly display on its website each available acceptance brand individually, so that the Cardholder may select Mastercard or Maestro independently of any other brand that may co-reside with Mastercard or Maestro.
2. If the Merchant has pre-selected an acceptance brand, the means for the Cardholder to override the Merchant's pre-selection must be presented in a clear and non-discriminatory manner.
3. The Cardholder's chosen acceptance brand must be respected and must not be converted to a different acceptance brand from that chosen by the Cardholder.

Digital Environment

By way of example but not limitation, the following requirements apply for Transactions completed in a **digital** environment, such as in-app Transactions and Transactions completed via a digital wallet:

1. A Customer, Merchant, Digital Wallet Operator, and Digital Activity Customer must provide the Cardholder a mechanism for selecting a default payment application for any co-badged Card provisioned in a Digital Wallet. If two Card images are displayed in the user interface, both must appear at the same time and the Cardholder must be required to choose between them. If a single Card image is displayed, the mechanism for choosing the default payment application must be clearly displayed and the Cardholder must be required to choose the default payment application via this mechanism. The Cardholder must be given a reasonable amount of time to select the default payment application. The default payment application must be selected only by the Cardholder, not pre-selected.
2. The Cardholder must be required to select a default payment application in the Digital Wallet during Card provisioning or at the time of Card activation. The Cardholder must be able to change the default payment application at any time. The Digital Wallet interface must not allow Card activation to be completed if the Cardholder has not selected a default payment application.
3. A user interface payment application selection method that is not already defined in the Corporation's specifications must be approved by the Corporation in writing before it is implemented.
4. The Cardholder's chosen payment application must be respected and must not be converted to a different payment application from that chosen by the Cardholder. Only the acceptance brand identifier of the payment application chosen by the Cardholder for the particular Transaction is to be sent to the Terminal.

Discrimination—SEPA Only, Excluding EEA Countries, Gibraltar, and the United Kingdom

In SEPA countries and territories that are neither EEA countries, nor Gibraltar, nor the United Kingdom, the Rule on this subject is modified as follows.

A Customer must not, directly or indirectly, prevent or discriminate against the use of Mastercard, Maestro, or Cirrus as a brand for Intracountry Transactions or Intra-SEPA Transactions. By way of example but not limitation:

1. A single certification must be valid for both intracountry and intra-SEPA use of a Mastercard, Maestro, or Cirrus Payment Application at the Terminal;
2. The prevalence of any particular chip-based payment application at the Terminal or Acquirer host system level must not be mandated or implemented;
3. If a Mastercard, Maestro, or Cirrus Payment Application is supported by both the Card and the Terminal, its use must not be blocked or impaired by technical or other means;
4. If a Mastercard, Maestro, or Cirrus Payment Application is supported by both the Card and the Terminal, the Cardholder must be given the opportunity to complete the Transaction with such Payment Application, in an EMV environment and in all other cases where the Terminal is technically capable of providing that choice to the Cardholder. In an EMV environment, if the Cardholder is not able to choose a payment application, the priority order defined by the Issuer in the chip must be respected.
5. Neither the Cardholder's chosen payment application nor the Issuer's priority order may be disregarded or overridden by technical or other means.

5.12.2 Charges to Cardholders

NOTE: Laws that permit Merchant surcharging may exist in particular countries. To the extent that such laws conflict with this Rule, they take precedence.

5.12.4 Scrip-dispensing Terminals

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

An Acquirer must not submit to the registered switch of its choice, any Transaction that arises from the acceptance of a Card at a scrip-dispensing Terminal.

5.12.5 Existing Cardholder Obligations

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

A Customer must not submit to the registered switch of its choice any Transaction that:

1. Represents the refinancing or transfer to a credit Card of an existing Mastercard Cardholder obligation that is deemed to be uncollectible; or
2. Arises from the dishonor of a Mastercard Cardholder's personal check.

6.1 Card Issuance—General Requirements

Region and Country Variations

In the Europe Region, the Rule on this subject is modified as follows.

1. Prior to 1 April 2024, a Card issued within **SEPA** must support both magnetic stripe and EMV chip technology, with the exception that a non-reloadable prepaid Card is not required to support EMV chip technology.
   Effective 1 April 2024:
   - A non-reloadable prepaid Card newly-issued within **SEPA** must support magnetic stripe or EMV chip technology or both.
   - All other Cards newly-issued within **SEPA** (excluding Switzerland) must support EMV chip technology and may support magnetic stripe technology.

   Effective 1 April 2029, a Card newly-issued within **SEPA** must support EMV chip technology and must omit magnetic stripe technology with the exception of a Card issued in Switzerland or a non-reloadable prepaid Card.

   Effective 1 April 2033, a Card issued (including those already issued) within **SEPA** must support EMV chip technology and must omit magnetic stripe technology with the exception of a Card issued in Switzerland or a non-reloadable prepaid Card.
2. All contactless Cards and Access Devices issued within **SEPA**, with the exception of the non-reloadable prepaid contactless Cards and Access Devices, must support EMV Mode Contactless Transactions.

3. Prior to 1 April 2024, all Cards issued in **Albania**, **Bosnia** and **Herzegovina**, **Kosovo**, **Moldova**, **Montenegro**, **North Macedonia**, or **Serbia** must support both magnetic stripe and EMV chip technology, with the exception that a non-reloadable prepaid Card is not required to support EMV chip technology.
   Effective 1 April 2024:

   – A non-reloadable prepaid Card newly-issued in **Albania**, **Bosnia** and **Herzegovina**, **Kosovo**, **Moldova**, **Montenegro**, **North Macedonia**, or **Serbia** must support magnetic stripe or EMV chip technology or both.
   – All other Cards newly-issued in **Albania**, **Bosnia** and **Herzegovina**, **Kosovo**, **Moldova**, **Montenegro**, **North Macedonia**, or **Serbia** must support EMV chip technology and may support magnetic stripe technology.

   Effective 1 April 2029, a Card newly-issued in **Albania**, **Bosnia** and **Herzegovina**, **Kosovo**, **Moldova**, **Montenegro**, **North Macedonia**, or **Serbia** must support EMV chip technology and must omit magnetic stripe technology with the exception of a non-reloadable prepaid Card.

   Effective 1 April 2033, all Cards issued (including those already issued) in **Albania**, **Bosnia** and **Herzegovina**, **Kosovo**, **Moldova**, **Montenegro**, **North Macedonia**, or **Serbia** must support EMV chip technology and must omit magnetic stripe technology with the exception of non-reloadable prepaid Cards.
4. All new and replacement contactless Access Devices, with the exception of non-reloadable prepaid Access Devices, must support EMV Mode Contactless Transactions.
5. All new and replacement contactless Cards, with the exception of non-reloadable prepaid Cards, must support EMV Mode Contactless Transactions ONLY.
6. All new and replacement contactless-enabled Access Devices issued on or after 1 April 2023 must support EMV Mode Contactless Transactions ONLY.
7. An Issuer in **Italy** must technically support and must not automatically decline Contactless Transactions on new and replacement Mastercard and Maestro Cards and Access Devices and on all Mastercard and Maestro Cards and Access Devices in circulation on or after 1 January 2022, with the exception of non-reloadable prepaid Cards and Access Devices.
8. An Issuer in **Italy** must personalize the chip on new and replacement Mastercard and Maestro Cards and Access Devices and on all Mastercard and Maestro Cards and Access Devices in circulation on or after 1 January 2022 (with the exception of non-reloadable prepaid Cards and Access Devices) to enable Contactless Transactions, including mandatory display of the EMVCo contactless indicator on the front of the Chip Card or Access Device.
9. The following requirements apply in **Albania, Austria, Bosnia, Bulgaria, Croatia, Czech Republic, Hungary, Israel, Montenegro, North Macedonia, Poland, Romania, Serbia, Slovakia, and Slovenia**:
   a. An Issuer must technically support ATM Transactions on its Contactless Cards and Access Devices. The Issuer must make individual authorization decisions and must not automatically decline ATM Transactions on its Contactless Cards and Access Devices.
   b. An Issuer must properly personalize the chip on its Contactless Cards and Access Devices that provide ATM access to enable contactless ATM Transactions.

EEA, Serbia, Bosnia and Herzegovina, Switzerland, Gibraltar, and the United Kingdom Variations

In the EEA, Serbia, Bosnia and Herzegovina, Switzerland, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

If a Card or Access Device is issued under a BIN or BIN range that has been allocated to the Corporation for Mastercard or Maestro issuance, and is co-badged with another payment scheme, the Mastercard or Maestro features and functionality must not be inferior to those of the other payment scheme.

By way of example but not limitation, such features and functionality include contactless support, activation in a Digital Wallet, and Tokenization.

A Chip Card newly issued under a BIN or BIN range that has been allocated to the Corporation for Mastercard or Maestro issuance must list the Mastercard or Maestro Payment Application associated with that BIN or BIN range with a level of priority not lower than any other chip application co-residing on the Card.

An Issuer in the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, or the United Kingdom, respectively, is responsible for accurately identifying the category (business/commercial, credit, debit, or prepaid) of each Mastercard and Maestro Card or Payment Application, in accordance with applicable regulation.

Transaction Alerts Service

The Transaction alerts service requirements set forth in Rule 6.1 of Chapter 6 apply with respect to a BIN or BIN range assigned for a Europe Region country as per the table below. The requirements in this modified Rule do not apply with respect to BINs or BIN ranges assigned for other Europe Region countries.

Country	Transaction Alerts Service Requirements Apply with Respect to the Following Card Types
United Kingdom and Ireland	Debit and Credit consumer Cards (Optional for Prepaid and Commercial Cards)
Andorra, Belgium, France, Gibraltar, Italy, Luxembourg, Monaco, Netherlands, Portugal, San Marino, Spain, Vatican City	Debit, Credit, and Prepaid consumer Cards and small/medium business Cards
Germany, Liechtenstein, Switzerland	Debit, Credit, and Prepaid consumer Cards and small/medium business consumer Cards. Maestro Cards are excluded.

The Transaction alerts service must:

- Provide the Cardholder with the option to activate a Transaction alerts service;
- Allow the activation of Transaction alerts by individual Account PAN;

- Deliver a Transaction alert to the Cardholder immediately upon approval of an authorization request for a Transaction that meets the parameters set by the Cardholder. The alert must indicate the Transaction date and time, Transaction type (for example, electronic commerce [e-commerce]), Transaction amount and currency, and Merchant name and country.
- Allow the Cardholder to set parameters for Transaction alerts based on authorization activity which, at a minimum, must include cross-border e-commerce Transactions, except in **Germany**, **Liechtenstein**, and **Switzerland**, where the parameters must include domestic as well as cross-border e-commerce Transactions, and except in the **United Kingdom** and **Ireland**, where the parameters must include, at a minimum:
  - Transaction amount
  - Cross-border Transactions
  - Transaction type (for example, e-commerce Transactions, mail order/telephone order [MO/TO] Transactions) or channel (for example, Card-not-present Transactions) or both.

Authentication Requirements—Europe Only

EMV 3DS and Identity Check

An Issuer must support the EMV 3DS specifications and Mastercard Identity Check and enroll all of its BIN ranges eligible for Remote Electronic Transactions in the new Mastercard authentication network.

Effective 14 October 2022, an Issuer must have enrolled all of its e-commerce-enabled Mastercard and Maestro BIN ranges in EMV 3DS 2.2. It must ensure, for itself and for its Service Providers (such as, ACS providers), the full implementation of EMV 3DS 2.2. In addition, an Issuer must ensure, for itself and for its Service Providers, the use of 3DS Requestor Initiated (3RI), and the EMV 3DS 2.2 authentication to Merchant app redirection (also called 3DS Requestor App URL).

Effective 14 October 2023, an Issuer must ensure, for itself and for its Service Providers, the use of Trusted Merchant Listing (TML).

An Issuer may implement alternative technical authentication solutions that provide equivalent authentication features and performance.

Issuer BIN ranges that already support EMV 3DS version 2.1 must continue to support this format and hence must be listed on the EMV 3DS version 2.1 Directory Server to ensure interoperability with Merchants that do not yet support EMV 3DS version 2.2 (such as, those outside of Europe).

In the **EEA, Gibraltar, United Kingdom, Switzerland, Andorra, Monaco, San Marino,** and **Vatican City**, an Issuer may implement alternative technical authentication solutions that are compliant with the Mastercard Identity Check Key Performance Indicators, which are published in the *Mastercard Identity Check Program Guide*.

An Issuer must be able to request SCA for each Remote Electronic Transaction. This requirement does not apply with respect to Cards issued under a BIN or BIN range assigned for **Switzerland** or to Cards for which the Issuer benefits from the exemption under Article 17 of the PSD2 (or corresponding legislation in other SCA Countries), for example lodged or virtual Corporate Cards.

It is recommended that an Issuer located in an SCA Country apply the exemptions from authentication that are permitted by applicable legislation, such as the Transaction Risk Analysis exemption, whenever the conditions for the application of such exemptions are met. It is recommended that an Issuer located in a country that is not an SCA Country apply Risk-Based Authentication.

Auto-Enrollment

An Issuer must auto-enroll new Cardholders and new and existing online banking users in the Identity Check Program or in its alternative SCA solution that is compliant with the PSD2 RTS requirements and the Mastercard Identity Check Key Performance Indicators, with regard to BINs assigned for any Europe Region country except for Germany, Liechtenstein or Switzerland, where auto-enrollment is recommended and not required.

An Issuer is not required to auto-enroll Cardholders of lodged or virtual Corporate Cards if the Issuer benefits from the exemption under Article 17 of the RTS.

Risk-Based Authentication

An Issuer in the following countries must have monitoring mechanisms in place to evaluate Remote Electronic Transactions for their level of risk and the need to require explicit authentication:

- Austria
- Bulgaria
- Croatia
- Czech Republic
- Cyprus
- Greece
- Hungary
- Malta
- Poland
- Romania
- Slovakia
- Slovenia

Biometrics

Except in the following countries, an Issuer must offer biometric authentication to Cardholders for Remote Electronic Transactions. An Issuer must also offer biometric authentication for Contactless Transactions carried out with a Mobile Payment Device at a POS Terminal. An Issuer is not required to offer biometric authentication on anonymous prepaid Cards or on lodged or virtual Corporate Cards if the Issuer benefits from the exemption under Article 17 of the RTS.

Support for biometric authentication is recommended and not required in the following countries:

- Albania

- Armenia
- Azerbaijan
- Belarus
- Bosnia and Herzegovina
- Georgia
- Israel
- Kazakhstan
- Kosovo
- Kyrgyzstan
- Montenegro
- North Macedonia
- Russian Federation
- Serbia
- Switzerland
- Tajikistan
- Turkey
- Turkmenistan
- Uzbekistan

A single mobile application must be usable for both Remote Electronic Transactions and for Contactless Transactions. The methods of biometric authentication must meet industry standards. It is recommended to offer at least two methods of biometric authentication as well as a fallback authentication method, such as a one-time password sent via SMS. Please refer to the *Mastercard European Biometric Authentication Standards Specification* for more information.

Mastercard Crypto Secure

The Rule on this subject does not apply to Issuers in Belarus, Italy, Russia, Switzerland, and Ukraine.

Mastercard Safety Net

In the Europe Region, the requirement for Issuers to participate in Mastercard Safety Net or Mastercard Safety Net alerts for non-Processed Transactions applies effective 12 December 2024, in the following countries only: Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, and Uzbekistan.

6.1.2 Maestro Card Issuance

In the Europe Region, the Rule on this subject is modified as follows.

A Chip Card must support online PIN verification as the CVM for Maestro Contactless Transactions that exceed the applicable Contactless Transaction CVM limit amount if online PIN is on the Card's CVM list for Contact Chip Transactions.

If the Card is issued under a BIN or BIN range assigned for a country in the EEA, Gibraltar, or the United Kingdom the Issuer is not required to maintain the funds in the Maestro Account, but must maintain the information necessary to process Transactions initiated by the Cardholder.

Additional requirements apply when the Maestro Account is funded from a source that is not the Issuer (for example, a payment card issued by a different issuer). See Rule 6.13 in this chapter for these additional requirements.

6.1.2.1 Eligible Accounts—Maestro

In the Europe Region, the Rule on this subject is replaced with the following:

Except in the EEA, Gibraltar, and the United Kingdom, a Maestro Card must be linked to a sight deposit account or to a pooled account (linked to a Corporation-approved prepaid Card Program). A Maestro Card may also be linked to a Mastercard credit Account in the context of a Corporation-approved multi-Account Card Program, if the account accessed via the Marks fulfills the requirement in the preceding sentence.

Cards issued under a BIN or BIN range assigned for a country in the EEA, Gibraltar, and the United Kingdom may be linked to any type of account (for example, credit and debit).

6.1.4 Tokenization of Accounts

In the EEA, Serbia, Bosnia and Herzegovina, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

If a Mastercard or Maestro Card or Access Device is co-badged with another payment scheme, and the other payment scheme is Tokenized, then the Mastercard or Maestro Card or Access Device must also be Tokenized.

Provisioning of Credentials into Click to Pay

Effective 14 October 2023, the following requirements apply to Issuers in Belgium, Czech Republic, Germany, Ireland, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland and the United Kingdom, that have more than 250,000 reported Mastercard consumer Accounts issued in the given country. Non-reloadable Prepaid, Commercial, and Maestro Accounts are excluded.

For Accounts issued under a BIN or BIN range assigned for any of the countries listed above, an Issuer must:

1. Technically support the provisioning of a Cardholder's Mastercard credentials into Click to Pay either via Mastercard's push provisioning product Token Connect or with the assistance of a Mastercard-approved third party;
2. Make the provisioning of credentials into Click to Pay available to the Cardholder at a minimum via the Issuer's mobile banking application; and
3. At time of online activation of newly issued, renewed, or replacement Mastercard Cards, make the provisioning of credentials into Click to Pay available to the Cardholder.

The Issuer must at a minimum prepopulate the cardholder name, account number and expiry date.

As a best practice, the Issuer should provide educational materials within its banking application regarding Click to Pay and the benefits of Click to Pay to Cardholders.

6.2 Issuer Responsibilities to Cardholders

In the Europe Region, the Rule on this subject is replaced with the following.

An Issuer must provide the following information to each of its Cardholders:

1. Before the Card is used, the Issuer must inform the Cardholder that the Card may be used wherever the Marks are displayed, and:
   a. The price of the Card;
   b. Specific charges, if any, to be paid to the Issuer for services provided through the Card or auxiliary charges applicable to the account, including but not limited to any Account access fees, cash advance fees, ATM usage fees, late payment fees, and interest rates to be applied;
   c. The basis for calculation of the exchange rate;
   d. Notice that exchange rates can fluctuate and that they may change between the time when the Transaction is made and the time when it is billed to the Cardholder's Account;
   e. The Cardholder's liability, including the cost, if the Card is lost or stolen. This information must be stated clearly in the body of the product literature. The Cardholder must also be told what to do if the Card is lost or stolen;
   f. The standard limit, if any, up to which the Cardholder can use the Card;
   g. When the Transaction is likely to be billed to the Cardholder's Account; and
   h. Information required to be provided by Rule 3.13.2 Data Subject Notice and Consent of this chapter.
2. At the time of billing the Transaction, as applicable, the following information must be provided to the Cardholder:
   a. Transaction type (for example, ATM cash withdrawal, cash advance) and location (if technically feasible);
   b. Amount in Transaction currency;
   c. Amount in billing currency;
   d. Exchange rate applied;
   e. Total commission applied (if applicable);
   f. Interest rate applied (if applicable).
3. Information relating to Changes to the Standards.
   An Issuer in the EEA, Gibraltar, or the United Kingdom must inform its Cardholders of any changes to the terms of the Cardholder agreement that result from changes made by the Corporation to the Standards. This information must be provided with at least two (2) months advance notice whenever possible.
4. Enhanced Merchant Data.
   Effective 14 October 2023, an Issuer in Albania, Andorra, Austria, Belgium, Bosnia, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Iceland, Ireland, Isle of Man, Italy, Jersey, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom or Vatican City must provide

to a Cardholder enhanced Merchant data, when available, to help the Cardholder recognize a Transaction when it is queried by the Cardholder. Such enhanced Merchant data includes, when available, without limitation, the Merchant's public facing or 'doing business as' name, location, contact details and logo. The Issuer must provide the enhanced Merchant data using the Issuer's banking application, mobile wallet, Internet banking interface, or other digital means that provides at least equivalent ease and accessibility for the Cardholder.

6.4 Selective Authorization

In the Europe Region, the Rule on this subject is modified as follows.

An Issuer may geographically restrict Maestro Card usage for a particular Maestro Card Portfolio as a fraud prevention measure, subject to the following requirements:

1. The geographic area in which the Card may be used must be clearly identifiable, for example domestic-only or Europe-only. For Cards issued in SEPA countries, a domestic-only restriction is not permitted.
2. The Issuer must use an Account range for the issuance of geographically restricted Cards that is separate from any Account range used for the issuance of unrestricted Cards, unless otherwise agreed with the Corporation.
3. The geographic restriction must be clearly printed on the Card front, for example "Valid only in Europe".
4. The Card design of geographically restricted Cards must be approved separately by the Corporation.
5. The Issuer must inform the Cardholder clearly in writing of the geographic scope of the Card and of any change in scope.
6. The Issuer must communicate the option of receiving a Card with no geographic restriction to all of its Cardholders and provide such a Card to any Cardholder who requests one.
7. The Issuer must obtain the Corporation's prior written approval of all Cardholder Communications.

6.5 Affinity and Co-Brand Card Programs

In the Europe Region, the Rule on this subject is modified as follows.

If a proposed A/CB Program will involve the addition of the Maestro and/or Cirrus Marks to cards carrying the logo of a domestic/local acceptance scheme in which the cards currently participate, the Corporation will approve the Program only if such scheme has already given its approval.

The Corporation reserves the right to require any Customer to submit all contracts with an A/CB Card Program Partner or any other documentation regarding an A/CB Card Program for purposes of determining compliance with the Standards.

6.10 Prepaid Card Programs

6.10.11 Simplified Due Diligence Guidelines

Refer to the *Prepaid Product Constructs* available on Mastercard Connect™ for additional information on simplified due diligence.

6.10.12 Debit Mastercard Meal/Food Voucher Card Programs

An issuer of a Prepaid Debit Mastercard Meal/Food Voucher Card program in the Czech Republic must ensure that no participation fees of any kind are charged directly by a program organizer to any Merchant participating in the program.

All other requirements for the prepaid product construct apply.

A meal/food voucher program not satisfying the above condition must not be issued as a Prepaid Debit Mastercard Meal/Food Voucher program.

6.11 Maestro Chip-only Card Programs

In the Europe Region, an Issuer may issue "Maestro Chip-only Cards," defined herein as Maestro Chip Cards for which the presence of a magnetic stripe is optional, or if the Card has a magnetic stripe, the magnetic stripe does not have a Maestro Payment Application, subject to the following conditions:

1. The Corporation must approve, in writing and in advance of Program launch, any Maestro Chip-only Card Program.
2. The Corporation must approve separately each Card design to be used in connection with a Maestro Chip-only Card Program.
3. The Account range used for a Maestro Chip-only Card Program must be separate from any Account range used for the issuance of other Maestro Cards, unless otherwise agreed with the Corporation.
4. The PAN on Maestro Chip-only Cards must not be embossed.
5. The optional magnetic stripe must not contain a payment application for any other brand.
6. In a Card-present environment, the Issuer must authorize solely Chip Transactions on a Maestro Chip-only Card.
7. The geographic scope of acceptance of a Maestro Chip-only Card Program must be limited to the Europe Region. The geographic restriction must be clearly printed on the Card front, for example "Valid only in Europe."
8. The Issuer must inform the Cardholder clearly in writing of the limitations on acceptance of the Card.
9. The Issuer must communicate the option of receiving an unrestricted Maestro Card to all Maestro Chip-only Card Program Cardholders and provide such a Card to any Cardholder who requests one.
10. The Issuer must submit and obtain the Corporation's prior written approval of all Cardholder Communications.

Effective 1 April 2024, the above Rules are withdrawn with the exception of subparagraph 5, which continues to apply for the period during which a Card is permitted to have an optional magnetic stripe.

6.12 Debit Card Programs Issued by Electronic Money Institutions and Payment Institutions

The Rules in this section apply to the issuance by an Electronic Money Institution or a Payment Institution in the EEA, Gibraltar, or the United Kingdom of a Debit Card Program.

6.12.1 Prior Consent of the Corporation

An Electronic Money Institution or Payment Institution must not conduct a Mastercard Debit or Debit Mastercard Card Program without the express prior consent of the Corporation.

Each request by an Electronic Money Institution or Payment Institution to conduct a Debit Card Program must be submitted to, and approved by, the Corporation via the Debit Program Registration process.

NOTE: Refer to the *Electronic Money Institution (EMI) and Payment Institution (PI) Debit Program Certification Form* on Mastercard Connect for additional information.

6.12.2 Reservation of Rights

The Corporation reserves the right to approve or reject any Debit Card Program application (and to require that any previously approved Debit Card Program be modified or terminated), if:

- The applicant does not have an Anti-Money Laundering (AML) program in compliance with the Mastercard Standards;
- The application does not meet the requirements stated in the Product Constructs above; or
- The application does not adhere to Mastercard Standards for Debit Mastercard or Mastercard Debit Card Programs.

A Customer may request that the Chief Franchise Officer of the Corporation review the rejection or withdrawal of the approval of a Debit Card Program. Such a request must be submitted in writing and signed by the Customer's Principal Contact. The request must be postmarked no later than 30 days after the date of receipt of the notice of rejection or withdrawal of approval. Any decision by the Chief Franchise Officer with respect to such rejection or withdrawal of approval is final and not subject to further review or other action.

6.13 Decoupled Payment Card Programs

The following additional Rules apply in the Europe Region.

A decoupled payment Card is a Card, other than a Prepaid Card, which is linked to a funding Card.

Decoupled payment Card Programs must only be issued under a BIN or BIN range assigned for an EEA country, Gibraltar, the United Kingdom or Russia.

NOTE: For specific Rules on loading Prepaid Accounts, refer to Rule 6.10.7, "Automatic Value Loads from Payment Cards," in Chapter 6 of this manual.

6.13.1 Prior Consent of the Corporation

A decoupled payment Card Program must not be issued without the express prior consent of the Corporation.

Each request to conduct a decoupled payment Card Program must be submitted to, and approved by, the Corporation via the Decoupled Payment Program Registration process before issuance begins.

6.13.2 Reservation of Rights

The Corporation reserves the right:

- To approve or reject any decoupled payment Card Program;
- To require that a previously approved decoupled payment Card Program be modified; and
- To withdraw approval of a decoupled payment Card Program and require it to be terminated.

A Customer may request that the Chief Franchise Officer of the Corporation review the rejection or withdrawal of approval of the decoupled payment Card Program. Such a request must be submitted in writing and signed by the Customer's principal contact. The request must be postmarked no later than 30 days after the date of receipt of the notice of rejection or withdrawal of approval. Any decision by the Chief Franchise Officer with respect to such rejection or withdrawal of approval is final and not subject to further review or other action.

6.13.3 AML Compliance

The decoupled payment Card Program must adhere to the Mastercard Anti-Money Laundering Standards, which require that each Customer conducting or proposing to conduct issuing and/or acquiring Activity must have policies, procedures, and controls in place to protect against the use of Mastercard systems for money laundering and terrorist financing. Refer to the Mastercard Anti-Money Laundering requirements in chapter 1 of this manual.

6.13.4 Selective Authorization Options

The decoupled payment Card Program must adhere to the *Selective Authorization Policy*.

6.13.5 Card Design Artwork

The decoupled payment Card Program must comply with the *Card Design Standards* and *Mastercard Brand Mark Guidelines*.

6.13.6 Lost/Stolen Reporting

The Issuer of the decoupled payment Card Program must ensure lost/stolen reporting to the Fraud and Loss Database.

6.13.7 Cardholder Access to Account Information

The decoupled payment Card Program must provide the Cardholder with access to balance inquiry and transaction history through the Internet, a call center, Interactive Voice Response Unit or other chosen methods of the Issuer.

6.13.8 Customer Service

The decoupled payment Card Program must provide access to live customer service.

6.13.9 Other Issuer Obligations

The Issuer of the decoupled payment Card Program must use a dedicated BIN or BIN range for the decoupled payment Card Program. No other Card Program is permitted to reside on the dedicated BIN or BIN range.

For a decoupled payment Card Program issued in the EEA, United Kingdom or Gibraltar, the funding source to which the Card is linked must be located in the EEA, United Kingdom or Gibraltar.

No Card issued under an anonymous or simplified due diligence construct may be used as a funding source. Refer to the *Prepaid Product Constructs and Guidelines for Anonymous Prepaid Card Programs*, available on Mastercard Connect, for more information.

The Issuer of the decoupled payment Card Program must inform the Cardholder how the Card functions when a payment is carried out, how the Card is loaded and the funding source. It must obtain the Cardholder's consent to the Card's method of operation.

The Issuer of the decoupled payment Card, as opposed to the funding source, is responsible for Activity, including Transactions, carried out on the Card.

The Issuer of the decoupled payment Card Program must inform the Cardholder that it, as opposed to the funding source, is the point of contact for all matters, including Cardholder inquiries or complaints related to the decoupled payment Card.

The Issuer of the decoupled payment Card Program is responsible for handling chargebacks of Transactions on the decoupled Card.

The Issuer of the decoupled payment Card Program will transfer amounts corresponding to refunds, chargebacks and reversals to the funding Issuer.

The zero-liability rule for unauthorized Transactions applies to decoupled payment Card Programs. Refer to Rule 6.3 in this manual.

Merchant Identification

The funding source must be informed, in DE 43 subfield 1 of the authorization request and the clearing message, of the decoupled Card Program name in conjunction with the name of the seller of the products/services purchased by the Cardholder; e.g. MERGE*Better shoes*, PRIMO *Coffee house*, etc.

Choice of MCC

The decoupled Card Program Issuer must pass to the funding Issuer the same MCC used to identify the business of the Merchant at which the decoupled Card is used to make a purchase.

If that MCC is assigned to a particular airline, vehicle rental, or lodging Merchant, then one of the following may be used, as applicable:

- MCC 4511 (Air Carriers, Airlines: Not Elsewhere Classified)
- MCC 7512 (Automobile Rental Agency: Not Elsewhere Classified)
- MCC 7011 (Lodging: Hotels, Motels, Resorts: Not Elsewhere Classified)

If the Transaction effected with the decoupled Card is an ATM Transaction or Manual Cash Disbursement Transaction, the repayment Transaction must be identified with MCC 6012 (Merchandise and Services: Customer Financial Institution).

A Funding Transaction MCC (i.e., MCCs 4829, 6538, or 6540) must only be used for the repayment Transaction if the decoupled Card is used for a Funding Transaction (in which case, the TTI and DE 108 data received must also be transmitted to the funding Issuer).

6.13.10 Rule Additions and Variations for Russia

The following Rule additions and variations apply for decoupled payment Card Programs in Russia.

Issuance of decoupled payment Card Programs is permitted on Mastercard BINs or BIN ranges only; Maestro, Cirrus and private label BINs are excluded.

The decoupled payment Card and the funding card may be issued by the same Issuer. The decoupled payment Card and associated funding card(s) must be issued by a Russian Issuer.

The Issuer of a decoupled payment Card must have performed full know your customer (KYC) due diligence, identification verification and sanctions screening on any prospective Cardholder before issuing a decoupled payment Card to the person.

The Cardholder for the decoupled Card must be the same as for the funding card. The decoupled Card Issuer bears responsibility for compliance with this requirement as well as with the requirement to ensure that the associated funding card(s) is issued by a Russian Issuer with a valid License.

Apart from the above restrictions, the decoupled payment Card Program Issuer must not block or discriminate against any Card as a funding source.

In the Transaction sent to the funding issuer, the generic decoupled Card Program name "DCP*" must be populated in DE 43, subfield 1, in front of the name of the seller of the products/services.

Partial funding of a Transaction made with a decoupled Card is not allowed; funding must not be split among multiple sources.

If a decoupled Card Program Issuer receives a Transaction processed to fund a Transaction on another Issuer's decoupled Card, such Funding Transaction must not be routed for further funding; tiering or looping of Transactions processed to funding cards is not permitted.

If a decoupled Card is used for a Cross-border Transaction, the Transaction charged to the funding card must nevertheless be processed in Russian rubles as the Transaction currency (the value 643 in DE 49) and the card acceptor country code specified in the Transaction charged to the funding card must indicate Russia (the value RUS in DE 43, subfield 5 of the authorization message; and in DE 43, subfield 6 of the clearing message).

7.1 Service Provider Categories and Descriptions

In the Europe Region, the "List of Services" column for "Third Party Processor (TPP)/TPP Program Service" Category / Program Service Name is modified to add the following.

7.1.1 Third Party Processor

In the Europe Region, the Rule on this subject is modified to add the following.

A TPP that performs switching services (authorization, clearing, settlement) must meet the minimum quality requirements established by the Corporation, as may be amended from time to time.

7.6 Acquiring Programs

7.6.5 Payment Facilitators and Submerchants

7.6.5.1 Responsibility for Payment Facilitator and Submerchant Activity

In the Europe Region, the Rule on this subject is modified as follows.

If a Submerchant is located in a country for which the Acquirer has central acquiring authorization in accordance with Rule 1.7.3, the Acquirer is not required to also obtain a License or an extension of its Area of Use covering the same country. If a Submerchant is located in a country that is not one of the Western or Central European countries listed in Rule 1.7.3.4, the central acquiring authorization must specifically mention the Submerchant.

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

An Acquirer must populate the Payment Facilitator ID and Submerchant ID in authorization and clearing messages in the fields specified by the registered switch of the Customer's choice.

7.6.6 Transaction Identification for ISO and PF Transactions

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

The ISO identification number must be provided in authorization and clearing messages in the field and with the value specified by the registered switch of the Customer's choice.

7.6.7 Staged Digital Wallet Operator Requirements

For Inter-European and Intra-European Transactions, item 3 of the global Rule is modified to add the following:

Cardholder dispute chargeback rights are also available for purchases of goods or services (excluding gambling, investments and similar provision of services) made using a Staged Digital Wallet, when the Staged Digital Wallet funding Transaction occurred during the consumer's purchase. With regard to gambling, investments and similar provision of services, only Cardholder dispute chargeback rights relating to the failure of funds to be loaded to the Staged Digital Wallet are available.

In the Europe Region, item 3(e) of the global Rule on this subject is modified as follows.

If a Staged DWO or a retailer receiving payment by means of a Staged DWO payment account is located in a country for which the Acquirer has central acquiring authorization, the Acquirer is not required to also obtain a License or an extension of such Acquirer's Area of Use covering the same country. If a Staged DWO or a retailer receiving payment by means of a Staged DWO payment account is located in a country that is not one of the Western or Central European countries listed in Rule 1.7.3.4, the central acquiring authorization must specifically mention the Staged DWO and/or retailer receiving payment by means of a Staged DWO payment account.

In the EEA, Gibraltar, and the United Kingdom, the following provisions in item 3 of the global Rule on this subject is modified as follows.

d. The Wallet Identification Number must be provided in authorization and clearing messages in the field and with the value specified by the registered switch of the Customer's choice.

g. The Staged DWO name must be provided in the field specified by the registered switch of the Customer's choice.

8.1 Definitions

In the Europe Region, the Rule on this subject is modified as follows.

"Interchange fee" is the fee that passes between the Acquirer and the Issuer with respect to the interchange of a Transaction conducted at a Merchant, the "purchase" part of a "purchase with cash back" Transaction or a Merchandise Transaction conducted at an ATM Terminal, including a chargeback, second presentment and reversal of such a Transaction.

"Service fee" is the fee that passes between the Acquirer and the Issuer with respect to the interchange of any other type of Transaction, including a Manual Cash Disbursement Transaction, ATM Transaction, "cash-back" part of a "purchase with cash back" Transaction,

refund, or Payment Transaction (such as MoneySend or Gaming Payment Transaction), including a chargeback, second presentment and reversal of such a Transaction.

8.2 Net Settlement

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

A Customer must refer to the documentation of the registered switch of its choice for currency conversion information.

8.2.1 Currency Conversion

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows.

A Customer must refer to the documentation of the registered switch of its choice for currency conversion information.

8.2.2 Settlement Messages and Instructions

The Corporation determines the net obligations of Customers under its Standards.

Customers' net obligations are calculated by the Corporation's proprietary small value clearing systems and are based upon accepted financial messages submitted by the Customers to the Interchange System. Such financial messages are irrevocable upon completion of the clearing system cutoff. A Customer may submit a subsequent financial message to modify a previously submitted financial message.

The Corporation subsequently creates instructions reflecting each Customer's end-of-day net obligations. Customers are required to effect funds transfers in accordance with these instructions, which result in the assumption or discharge of payment obligations between Customers.

For additional information regarding settlement finality and discharge of settlement obligations following an instruction, see the *Settlement Manual*.

8.2.2.1 Cooperation with Government Authorities

Each Europe Region Customer agrees and acknowledges that, for the purposes of administering the Interchange System, the Corporation may from time to time co-operate (by sharing of information or otherwise) with:

1. The Financial Services Authority;
2. The Bank of England;
3. Any relevant office holder (as defined in the UK SFD Regulations); and
4. Any authority, body or person having responsibility for any matter arising out of, or connected with, the default of a Customer.

8.2.2.2 Provision of Information

For the purposes of the UK SFD Regulations, each Europe Region Customer must (except if such request is frivolous or vexatious) provide to any interested person who requests it, within 14 days of such request and upon payment by such a person of a reasonable charge.

1. Details of the systems which are designated for the purposes of the Settlement Finality Directive in which such Customer participates; and
2. Information about the main rules governing the functioning of such systems.

8.2.2.3 Notification of Winding Up Resolution or Trust Deed

For the purposes of the UK SFD Regulations, each Europe Region Customer must (i) upon the passing of a creditor's voluntary winding up resolution (or analogous procedure in the jurisdiction of incorporation of such Customer) in respect of that Customer; or (ii) upon a trust deed granted by the Customer becoming a protected trust deed, notify the Corporation and the Bank of England that such a resolution (or analogous procedure) has been passed or that such a trust deed has become a protected trust deed, as the case may be.

8.3 Interchange and Service Fees

In the Europe Region, the Rule on this subject is modified as follows.

Detailed information on how interchange fees are applied in the Europe Region is contained in the *Interchange Manual—Europe Region*. An Acquirer must submit Transactions completed at Merchants with the interchange rate designator for the lowest fee tier applicable to them.

8.4 Establishment of Intracountry Interchange and Service Fees

8.4.2 Bilateral Agreement

Bilaterally agreed interchange fees applicable to Intracountry Transactions in Andorra, Gibraltar, Serbia, Bosnia and Herzegovina, and the United Kingdom, and in EEA countries, to Transactions between Andorra and an EEA country, and to Intra-EEA Transactions must not exceed the maximums set pursuant to applicable law or regulation.

8.5 Failure of a Principal or Association to Discharge a Settlement Obligation

In the EEA, Gibraltar, and the United Kingdom, the Rule on this subject is modified as follows:

The term "Corporation" is replaced by "Mastercard International Incorporated." For further clarification, Mastercard Europe facilitates application of this Rule to Customers in the EEA, Gibraltar, and the United Kingdom and manages Customer interactions related to this Rule,

including validation of claims. Mastercard International Incorporated has full responsibility and liability for payment of valid claims made pursuant to this Rule.

8.8 System Liquidity

In the Europe Region, the Rule on this subject is modified as follows.

Customers will be informed at least 48 hours in advance, unless exceptional circumstances warrant a faster execution, for each day that the Corporation collects funds.

8.11 Loss Allocation Among Customers

In the Europe Region, the following additional Rule applies.

Any losses incurred by the Corporation, or for which the Corporation may otherwise be responsible due to the failure of a Maestro Customer to perform its settlement obligations, will be apportioned among Maestro Customers in the Region.

Without prejudice to the Corporation's rights under Rule 8.11 in Chapter 8 of these Rules, the apportionment of losses will be based on (amongst other things) Customers' guaranteed issuing and acquiring Volumes. The collection of the loss allocation will be undertaken by the Corporation as soon as practicable under the circumstances of the settlement losses and may be carried out over an extended period if required.

Chapter 14 Latin America and the Caribbean Region

This chapter contains Rules pertaining to Activity conducted in the Latin America and the Caribbean Region.

Applicability of Rules

The Rules in this Latin America and the Caribbean Region chapter are variances and additions to the "global" Rules that apply in the Latin America and the Caribbean Region or in a particular Region country or countries.

Refer to Appendix A for the Latin America and the Caribbean Region geographic listing.

Definitions

Solely within Brazil, the following terms have the meanings set forth below:

Maestro Contactless Magnetic Stripe Transaction

A Maestro POS Transaction initiated by a Cardholder with a Card issued in Brazil at a Merchant located in Brazil, and which contains a value of 91 in Data Element (DE) 22 (Point of Service Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), data field position 1–2 and a value of 3 or 4 in DE 61 (Point of Service [POS] Data), subfield 11 (POS Card Data Terminal Input Capability Indicator).

3.1 Obligation to Issue Mastercard Cards

In the Latin America and the Caribbean Region, the Rule on this subject is modified to include the following:

A Customer that is Licensed to acquire Transactions in the United States that extends its Area of Use to acquire Transactions in Puerto Rico is not required to issue Mastercard Cards in Puerto Rico if its acquiring Activity in Puerto Rico is limited to only the Transactions of Merchants located in Puerto Rico that are also located and have headquarters in the United States, and with whom the Customer has an existing acquiring relationship in the United States.

3.13 Privacy and Data Protection

A Customer that is subject to Brazil Data Protection Law must comply with both Rule 3.13 as set forth in Chapter 3, "Customers Obligations", and this Rule 3.13, which applies to Processing of Personal Data subject to Brazil Data Protection Law.

As used in this Rule, the following terms have the meanings as described below.

Brazil Data Protection Law

Any law, statute, declaration, decree, legislation, enactment, order, ordinance, directive, regulation or rule (as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which the Corporation and the

Customer are subject in Brazil, including but not limited to the Brazil General Data Protection Act (Law 13.709/2018).

Controller

The entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to or other unauthorized Processing of Personal Data transmitted, stored, or otherwise Processed.

Processor

The entity which Processes Personal Data on behalf of a Controller.

Sensitive Data

Any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to Brazil Data Protection Law.

Sub-Processor

The entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

3.13.8.1 Processing for Purposes of Activity and Digital Activity

In Brazil, Rule 3.13.1 is modified to include the following.

A Customer is a Controller with regard to the Processing of Personal Data for the purposes of carrying out the Customer's Activities and Digital Activities, and the Corporation acts as a Processor for these purposes.

Each Customer acknowledges that the Corporation may Process, as a Controller, Personal Data for the purposes of accounting, auditing and billing; fraud, financial crime and risk management; defense against claims, litigation and other liabilities; arbitration and other decisions relating to dispute resolution; product development and improvement; internal research, reporting and analysis; anonymization of data to develop data analytics products; and compliance with legal obligations. The Corporation represents and warrants that it will Process Personal Data for these purposes in compliance with Brazil Data Protection Law and the Standards.

To the extent that it acts as a Processor, the Corporation will: (1) cooperate with Customers in their role as Controllers to fulfill their data protection compliance obligations in accordance with Brazil Data Protection Law; (2) only undertake Processing of Personal Data in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in the Standards or as otherwise agreed in writing; and (3) comply with obligations equivalent

to those imposed on the Customers as Controllers by the applicable provisions of Brazil Data Protection Law, including those applicable to Processors and data transfers.

The Corporation will notify the Customer when local laws prevent the Corporation from (1) complying with the Customer's instructions (except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), and (2) from fulfilling its obligations under the Standards and have a substantial adverse effect on the guarantees provided by the Standards.

3.13.8.2 Data Subject Notice and Consent

In Brazil, Rule 3.13.2 is modified to include the following.

A Customer must ensure that the Processing of Personal Data for the purposes provided in Rule 3.13.1 relies on a valid legal ground under Brazil Data Protection Law, including obtaining Data Subjects' proper consent where required or appropriate under Brazil Protection Law.

A Customer must ensure that Data Subjects receive appropriate notice, in a timely manner: (1) with at the minimum all of the elements required under Brazil Data Protection Law, and (2) about the existence of Processors located outside of Brazil.

3.13.8.3 Data Subject Rights

In Brazil, Rule 3.13.3 is modified to include the following.

A Customer must develop and implement appropriate procedures for handling Data Subjects' requests to exercise their rights under Brazil Data Protection Law, including, as applicable, the right of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing of Personal Data, (f) objection, and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them.

To the extent that the Corporation acts as a Processor, the Corporation will assist the Customer in complying with its obligation to respond to such requests, including by providing access to Personal Data maintained by the Corporation.

3.13.8.4 Accountability

Taking into account the nature, scope, context, and purposes of Processing of Personal Data, as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, the Corporation and the Customers must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that Processing of Personal Data is performed in accordance with the Standards and Brazil Data Protection Law, including, as applicable, by appointing a data protection officer, maintaining records of Processing of Personal Data, complying with the principles of data protection by design and by default, performing data protection impact assessments, and conducting prior consultations with supervisory authorities. The Corporation will cooperate with the Customer to ensure compliance with and to assist the Customer in fulfilling their own obligations under Brazil Data Protection Law.

3.13.8.5 International Data Transfers

Each Customer authorizes the Corporation to transfer Personal Data Processed subject to Brazil Data Protection Law outside of Brazil in accordance with Brazil Data Protection Law.

3.13.8.6 Sub-Processing

In Brazil, Rule 3.13.6 is modified to include the following.

To the extent that the Corporation acts as a Processor, the Customer gives a general authorization to the Corporation to use internal and external Sub-Processors on its behalf.

The Corporation requires its Sub-Processors, using a written agreement, to comply with the requirements of Brazil Data Protection Law, with the Customers' instructions, and with the same obligations as are imposed on the Corporation by the Standards.

3.13.8.7 Disclosures of Personal Data

Where the Corporation is requested to disclose Personal Data to a law enforcement authority or state security body ("Requesting Agency") that the Corporation is Processing, the Corporation will only comply with such request in accordance with Brazil Data Protection Law. Where the Corporation is acting as a Processor, the Corporation will refer the Requesting Agency to the Customer, unless the Corporation is prohibited from doing so.

3.13.8.8 Security and Data Protection Audit

In accordance with the Standards and Brazil Data Protection Law, the Corporation and each Customer must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate level of security, the Corporation and the Customer must take into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of Processing of Personal Data, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

The Corporation and each Customer must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and as applicable Processes Personal Data in accordance with the Customer's instructions.

3.13.8.9 Personal Data Breaches

Where the Corporation acts as a Processor, and where required under Brazil Data Protection Law, the Corporation will inform the Customer, without undue delay, of a Personal Data Breach.

The Corporation will assist the Customer in complying with its own obligations to notify a Personal Data Breach. The Corporation and each Customer must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects, and the remedial action taken.

3.13.8.10 Liability for Brazil Data Protection Law Violations

Where the Customer or the Corporation acts as a Controller, it is responsible for the damage caused by the Processing of Personal Data which infringes Brazil Data Protection Law or these Standards. To the extent that the Corporation acts as a Processor, it will be liable for the damage caused by Processing of Personal Data only where it has not complied with obligations of Brazil Data Protection Law specifically directed to Processors or where it has acted outside or contrary to lawful instructions of the Controller. The Corporation will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where one or more Customers and/or the Corporation are involved in the same Processing of Personal Data and where they are responsible for any damage caused by Processing of Personal Data, each may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If the Corporation paid full compensation for the damage suffered, it is entitled to claim back from the Customer(s) involved in the same Processing of Personal Data that part of the compensation corresponding to their part of responsibility for the damage.

4.8 Use of Marks on Maestro and Cirrus Cards

In Brazil, the Rule on this subject as it applies in Brazil is modified as follows.

1. The Marks may be placed on cards in combination with other local/international ATM marks.
2. The Marks may co-reside on a Mastercard Card in the context of a multi-Account Card Program.
3. A Customer must not place local/regional POS debit marks on Maestro Cards bearing the Marks and must be in full compliance with Rule 4.9, as may be amended from time to time.
4. The Marks may not be placed on any debit card that does not qualify as a Maestro Card.

5.8 Transaction Message Data

5.8.6 Enablement of QR-based Payments

The following Rule applies in Argentina.

If a QR provider (whether a Merchant, its Acquirer, or the Acquirer's Payment Facilitator or other Service Provider) has enabled a Merchant located in Argentina to accept payments via the display of a QR code that can be parsed by a third-party (non-proprietary) digital wallet or mobile payment application, then:

- The QR code must be compliant with the EMV QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode standard; and
- The QR provider must be able to receive Card credentials transmitted by such third-party digital wallet or mobile payment application and use the Card credentials to effect a Transaction in accordance with the Standards.

5.11 Merchant Obligations for Acceptance

5.11.5 Discounts or Other Benefits at the Point of Interaction

In the Latin America and the Caribbean Region, a discount or other benefit may be applied at the POI upon presentation of a particular Mastercard Card or Maestro Card for payment.

The Merchant may promote such discount or other benefit at the POI location, provided such promotion does not disparage other Card Programs.

6.1 Card Issuance—General Requirements

Transaction Alerts Service

In the Latin America and the Caribbean Region, the Issuer's offering of a Transaction alerts service is required for commercial Cards issued for use by a small or mid-sized business (as defined by the Corporation).

Mastercard Crypto Secure

The Rule on this subject does not apply to Issuers in Brazil, Dominican Republic, and Mexico.

Mastercard Safety Net

In the Latin America and the Caribbean Region, the requirement for Issuers to participate in Mastercard Safety Net or Mastercard Safety Net alerts for non-Processed Transactions does not apply.

6.1.2 Maestro Card Issuance

In the Latin America and the Caribbean Region, the Rule on this subject as it applies in Brazil, Chile, and Colombia is modified as follows.

In Brazil, Chile, and Colombia, a Chip Card must support online PIN verification as the CVM for any Contactless Transaction initiated with a Card issued in Brazil, Chile, or Colombia that exceeds the Contactless Transaction CVM limit amount. In Brazil, this Rule applies to both Maestro Contactless Transactions and Maestro Contactless Magnetic Stripe Transactions.

8.2 Net Settlement

8.2.1 Currency Conversion

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

With respect to Mastercard POS Transactions occurring within the country in which the Mastercard Account was issued, if that country is within the Region, and if the Transaction currency is the same as the currency of the Issuer and is not U.S. dollars, the Acquirer must accept payment for the Transaction in the local currency, unless the Acquirer and Issuer have agreed otherwise, or unless local law requires otherwise.

Noncompliance by any Customer with this requirement will result in the imposition of a USD 50 assessment for each USD 1,000 of affected settlement volume, payable monthly for the volume in the prior month.

8.4 Establishment of Intracountry Interchange and Service Fees

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

Integrated Service for Intracurrency Settlement (ISIS) certification is a standard feature of the certification process for Mastercard Programs in which a Region Customer participates. All Principals and Associations in the Region and Service Providers providing Program Services to Principals and Associations in the Region must settle Mastercard POS Transactions through ISIS at the applicable intracountry interchange rate and conditions with each Region Customer that chooses to use ISIS as its settlement platform for Intracountry POS Transactions.

8.5 Failure of a Principal or Association to Discharge a Settlement Obligation

In Venezuela, the Rule on this subject is modified as follows.

Subject to the limitation set forth in this Rule, if a Principal or Association fails to discharge a Settlement Obligation arising from or in connection with any Processed Transaction, Mastercard Spain Holdings, S.L. will satisfy such Settlement Obligation to the extent such Settlement Obligation is not otherwise satisfied.

To the extent that Mastercard Spain Holdings, S.L. satisfies a Customer's Settlement Obligation, such satisfaction constitutes an automatic transfer, sale, and absolute assignment to Mastercard Spain Holdings, S.L., and not an assignment for security purposes, of all right, title, and interest in the receivable. Such satisfaction of the Customer's Settlement Obligation also entitles the Corporation to all records and documents related to the receivable, including the name and address of each Cardholder or other person obligated to satisfy any part of the receivable. The Customer must promptly deliver all such records and documents to the Corporation or to the Corporation's designee. Any proceeds received by or on behalf of the

Customer from any receivable must be held in trust by the Customer and paid to the Corporation as soon as practicable.

The Corporation may take any action that the Corporation deems necessary or appropriate to protect the receivable and to protect the integrity of the affairs of the Corporation, such as, by way of example and not limitation, by:

1. Refusing or rejecting Transaction authorization requests relating to use of the Customer's Cards or refusing or rejecting PTA Transaction initiation requests.
2. Without prior notice to the Customer, holding any monies due, directly or indirectly and for any purpose, to the Customer from the Corporation and any Settlement Obligations due to the Customer and apply those monies to the amounts that the Customer owes to the Corporation and to other Customers arising from Activity.
3. Listing some or all of a Customer's Account numbers on the Electronic Warning Bulletin file, the international Warning Notices, or both, or in other or similar publications.
4. Effecting chargebacks on behalf of the Customer.
5. Overseeing the disposition of unused Card stock and any other media bearing security sensitive information, including Account information.

Mastercard Spain Holdings, S.L. assumes no liability, responsibility, or obligation to satisfy, in full or in part:

A. A Settlement Obligation arising from or in connection with a Transaction that was not a Processed Transaction.

B. A Settlement Obligation arising from or in connection with a Transaction in which the Principal or Association, considered together with one or more of its Affiliates, acts as both the Issuer and the Acquirer.

C. A Settlement Obligation arising from or in connection with a Transaction in which the Issuer and Acquirer are related parties or are under common Control by one or more parents, holding companies, or other entities.

D. A Settlement Obligation arising from or in connection with any of the Principal's or Association's Sponsored Affiliates.

E. A Settlement Obligation arising from or in connection with an Intracountry Transaction that was not settled, in whole or in part, where the non-settlement was expressly directed, mandated, or otherwise compelled by a government or governmental regulatory agency, regardless of whether such direction or mandate was publicly announced. For clarity, this provision shall not apply where the non-settlement occurred at the direction of a government or government-designated receiver or trustee made in the ordinary course of a receivership/insolvency proceeding.

Payment Transfer Activity Variation

In Venezuela, the Rule on this subject, as it applies to Payment Transfer Activity for a PTA Settlement Guarantee Covered Program, is revised and restated as follows.

Subject to the limitation set forth in this Rule, if a Principal or Association Originating Institution fails to discharge a PTA Settlement Obligation arising from or in connection with any first presentment Processed PTA Transaction for a PTA Settlement Guarantee Covered Program, Mastercard Spain Holdings, S.L. will satisfy such PTA Settlement Obligation to the extent such PTA Settlement Obligation is not otherwise satisfied.

To the extent Mastercard Spain Holdings, S.L. satisfies an Originating Institution's PTA Settlement Obligation, such satisfaction constitutes an automatic transfer, sale, and absolute assignment to Mastercard Spain Holdings, S.L., and not an assignment for security purposes, of all right, title, and interest in the receivable. Such satisfaction of the Originating Institution's PTA Settlement Obligation also entitles the Corporation to all records and documents related to the receivable, including the name and address of each Account Holder or other person obligated to satisfy any part of the receivable. The Originating Institution must promptly deliver all such records and documents to the Corporation or to the Corporation's designee. Any proceeds received by or on behalf of the Originating Institution from any receivable must be held in trust by the Originating Institution and paid to the Corporation as soon as practicable.

The Corporation may take any action that the Corporation deems necessary or appropriate to protect the receivable and to protect the integrity of the affairs of the Corporation, such as, by way of example and not limitation, by:

1. Refusing or rejecting PTA Transaction initiation requests or refusing or rejecting any Transaction authorization requests relating to use of the Customer's Cards.
2. Without prior notice to the Originating Institution, holding any monies due, directly or indirectly and for any purpose, to the Originating Institution from the Corporation and any PTA Settlement Obligations due to the Originating Institution and apply those monies to the amounts that the Originating Institution owes to the Corporation and to other PTA Customers.
3. Listing some or all of the PTA Account Numbers held by or on behalf of such Originating Institution on the Electronic Warning Bulletin file, the international Warning Notices, or both, or in other or similar publications.
4. Effecting chargebacks on behalf of an affected PTA Customer, if available.
5. Overseeing the disposition of any media bearing security sensitive information, including PTA Account information.

Mastercard Spain Holdings, S.L. assumes no liability, responsibility, or obligation to satisfy, in full or in part:

A. A PTA Settlement Obligation arising from or in connection with a PTA Transaction that was not a Processed PTA Transaction.

B. A PTA Settlement Obligation arising from or in connection with a PTA Transaction in which the PTA Customer, considered together with one or more of its Affiliates, acts as both the Originating Institution and the Receiving Customer.

C. A PTA Settlement Obligation arising from or in connection with a PTA Transaction in which the Originating Institution and the Receiving Customer are related parties or are under common Control by one or more parents, holding companies, or other entities.

D. A PTA Settlement Obligation arising from or in connection with any of the PTA Customer's Principal's or Association's Sponsored Affiliates.

E. A PTA Settlement Obligation arising from or in connection with a PTA Transaction that was not settled, in whole or in part, where the non-settlement was expressly directed, mandated, or otherwise compelled by a government or governmental regulatory agency, regardless of whether such direction or mandate was publicly announced. For clarity, this provision shall not apply where the non-settlement occurred at the direction of a government or government-designated receiver or trustee made in the ordinary course of a receivership/insolvency proceeding.

8.11 Loss Allocation Among Customers

In the Latin America and the Caribbean Region, the Rule on this subject is modified as follows.

Any losses that the Corporation incurs, or for which the Corporation may otherwise be responsible due to the failure of a Maestro Customer to perform its Customer obligations, will be allocated to the Maestro Principals in the Region. The allocation will be determined by the Corporation or in accordance with expense allocation practices in effect at that time, whether regional, global, operational, or any other.

The Corporation will determine the timing of the collection, which will be as immediate as is practicable, but may be carried out over an extended period if deemed necessary or appropriate.

9.2 DWO Requirements—Pass-through Digital Wallet

9.2.8 Enablement of QR-based Payments

The following Rule applies in Argentina.

If a Pass-through Digital Wallet is able to support a domestic Quick Response (QR)-based payment method offered in Argentina, then the DWO must:

- Ensure its mobile application can scan and parse a QR code containing Mastercard payload information, in accordance with the EMV QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode standards; and
- Offer Cardholders the option to store and select a Card as the payment method for any QR-based payments.

Chapter 15 Middle East/Africa Region

This chapter contains Rules pertaining to Activity conducted in the Middle East/Africa Region.

Applicability of Rules

The Rules in this Middle East/Africa Region chapter are variances and additions to the "global" Rules that apply in the Middle East/Africa Region or in a particular Region country or countries.

Refer to Appendix A for the Middle East/Africa geographic listings.

Definitions

Solely within South Africa, the following terms have the meanings set forth below:

Debit, Debit Mastercard Card, Debit Card

Any Mastercard Card or Program issued in South Africa, by a Customer licensed in South Africa, that when presented for payment in South Africa, accesses, debits, holds, or settles funds from a consumer's deposit, current, saving, asset or other type of money account. "Debit" or "Debit Mastercard Card" shall include consumer signature and/or PIN debit Programs, stored value Programs, prepaid Cards, payroll Cards and electronic benefit transfer Cards.

Other Mastercard Card

Any Mastercard Card or Program issued in South Africa that is not defined as "debit" or "Debit Mastercard Card."

Solely within the MEA Region, the following terms have the meanings set forth below:

Intra-UEMOA Transaction

A Transaction that is not an Intracountry Transaction and that is completed using a Card issued in a country or territory that is part of the UEMOA at a Terminal located in a country or territory that is part of the UEMOA and that is acquired by an Acquirer pursuant to a License for a country or territory that is part of the UEMOA.

West African Economic and Monetary Union (UEMOA)

The following countries, islands and territories: Burkina Faso, Cote d'Ivoire, Mali, Niger, Senegal, Benin, Guinea Bissau and Togo.

1.7 Area of Use of the License

In the MEA Region, the Rule on this subject is modified as follows.

In the UEMOA, the License covers the entire UEMOA as the Area of Use.

A separate ICA is required for ATM acquiring in each UEMOA country. A separate ICA and BIN or BIN range is required for issuance in each UEMOA country.

Different ranges within a BIN assigned to an Issuer may be linked to ICAs assigned to that same Issuer for different countries. A Customer is not required to have a physical establishment in the Area of Use.

1.7.1 Extending the Area of Use

In all countries of the Middle East/Africa Region, the Rule on this subject is modified as follows.

A Principal Customer may apply for an extension to its Area of Use to sponsor an entity that is located in a country different from the country in which the Principal Customer is incorporated or is otherwise constituted. The Corporation may at its absolute discretion grant to a Principal Customer such an extension of its Area of Use if such an extension brings sufficient value to the Corporation.

What constitutes sufficient value is to be determined solely by the Corporation. In addition to bringing sufficient value to the Corporation, all of the following conditions must be met at all times:

1. The Principal Customer is:
   a. Licensed in at least one country listed in the Middle East/Africa geographic listing in Appendix A; and
   b. At all times compliant with PCI Security Standards for Level 1 Service Providers as described in section 2.2.3, "Service Provider Compliance Requirements," of the *Security Rules and Procedures* manual.
2. The entity proposed to be Sponsored:
   a. Must be incorporated or is otherwise constituted in a country located in one of the countries or territories listed in the Middle East/Africa geographic listing in Appendix A;
   b. Is a financial institution authorized to engage in Activity under the laws or government regulations of the country in which it is incorporated or is otherwise constituted;
   c. Engages in Activity within six months of becoming an Affiliate Customer;
   d. Limits its Activity to the country in which it is incorporated or is otherwise constituted after it becomes an Affiliate Customer; and
   e. Must not be sponsored by more than one Principal Customer.
3. The Principal Customer and Affiliate Customer each agree that all Transactions conducted pursuant to such an extension must be authorized, cleared and settled through the Interchange System of the Corporation.
4. The total Mastercard gross dollar volume (GDV) of an Affiliate Customer must not exceed 15 percent of the total GDV of the Corporation in that country. An Affiliate Customer will be required to apply to become a Principal Customer if it exceeds this 15 percent threshold.

For Customers that have a License for the UEMOA, the Rule on this subject is modified as follows.

A Principal or Association Customer may apply for an extension of its Area of Use to Sponsor an entity that is located in a country different from the country in which the Principal or Association Customer is incorporated or otherwise constituted.

The entity proposed to be Sponsored:

a. Must be authorized to engage in Activity under the laws or government regulations of an UEMOA country;

b. Must limit its Activity to the Area of Use mentioned in its License.

1.7.2 Extension of Area of Use Programs

A Customer with a License for the UEMOA is not required to apply for an extension of Area of Use in order to undertake Activity in an additional country within the UEMOA.

3.1 Obligation to Issue Mastercard Cards

The Rule on this subject does not apply in South Africa.

5.1 The Merchant and ATM Owner Agreements

5.1.2 Required Merchant Agreement Terms

In South Africa, the Rule on this subject is modified as follows.

With respect to Mastercard Card acceptance in South Africa, a Merchant Agreement must provide the Merchant with the options, and the applicable Merchant discount rate for each option, to elect to accept South Africa-issued Debit Mastercard Cards only, South Africa-issued Other Mastercard Cards only, or both South Africa-issued Debit Mastercard Cards and South Africa-issued Other Mastercard Cards. A Merchant may choose to stop accepting South Africa-issued Debit Mastercard Cards or South Africa-issued Other Mastercard Cards by providing no less than 30 days advance written notice to its Acquirer.

5.11 Merchant Obligations for Card Acceptance

5.11.1 Honor All Cards

In South Africa, the Rule on this subject, as it applies to the acceptance of Mastercard Cards issued in South Africa, is replaced with the following:

1. **Honor All Debit Mastercard Cards.** Merchants that choose to accept Debit Mastercard Cards must honor all valid Debit Mastercard Cards without discrimination when properly presented for payment. The Merchant must maintain a policy that does not discriminate among customers seeking to make purchases with a Debit Mastercard Card.
2. **Honor All Other Mastercard Cards.** Merchants that choose to accept Other Mastercard Cards must honor all Other Mastercard Cards without discrimination when properly presented for payment. The Merchant must maintain a policy that does not discriminate among customers seeking to make purchases with another Card.

5.11.2 Merchant Acceptance of Mastercard Cards

In South Africa, the following Rule applies to the acceptance of Mastercard Cards issued in South Africa:

A Merchant in South Africa that accepts Mastercard Cards may choose to accept Debit Mastercard Cards only, Other Mastercard Cards only, or both Debit Mastercard Cards and Other Mastercard Cards. The Acquirer must advise the Corporation when a Merchant chooses not to accept either Debit Mastercard Cards or Other Mastercard Cards.

Merchants may request signage for the purpose of indicating their acceptance of Debit Mastercard Cards at www.mastercardweacceptdebit.com. An Acquirer must provide a complete list of accurate and current BINs obtained through the Corporation that apply to Debit Mastercard Cards to its Merchants and ensure that its Merchants use the updated BIN information within six calendar days of such file being made available by the Corporation.

5.11.5 Discounts or Other Benefits at the Point of Interaction

In the Middle East/Africa Region, a discount or other benefit may be applied at the POI upon presentation of a particular Mastercard Card for payment.

Promotion of any such discount or other POI benefit is permitted provided such promotion does not result in discrimination against other Card Programs. The determination of whether any promotion discriminates against other Card Programs is at the sole discretion of the Corporation.

6.1 Card Issuance—General Requirements

Transaction Alerts Service

In the Middle East/Africa Region, the Issuer's offering of a Transaction alerts service is required for commercial Cards issued for use by a small or mid-sized business (as defined by the Corporation).

Mastercard Crypto Secure

The Rule on this subject does not apply to Issuers in Jordan.

Mastercard Safety Net

In the Middle East/Africa Region, the requirement for Issuers to participate in Mastercard Safety Net or Mastercard Safety Net alerts for non-Processed Transactions applies:

- Effective 30 June 2023 in Afghanistan, Bahrain, Benin, Burkina Faso, Burundi, Central African Republic, Chad, Comoros, Ethiopia, Gabon, Iraq, Lebanon, Lesotho, Madagascar, Malawi, Namibia, Palestine, Seychelles, Swaziland, Zambia, and Zimbabwe;
- Effective 12 December 2023 in Algeria, Cameroon, Congo, Cote D'Ivoire, Democratic Republic of the Congo, Djibouti, Equatorial Guinea, Gambia, Ghana, Guinea, Kenya, Liberia,

Libya, Mali, Mauritania, Niger, Rwanda, Senegal, Sierra Leone, Somalia, South Africa, South Sudan, Togo, Uganda, and Yemen; and

- Effective 30 June 2024 in Cape Verde, Egypt, Kuwait, Morocco, Pakistan, Qatar, Mauritius, Mozambique, Saudi Arabia, Tanzania, Tunisia, and United Arab Emirates.

6.1.1 Mastercard Card Issuance

In South Africa, the Rule on this subject is modified as follows.

An Issuer must use specific and unique bank identification numbers (BINs) for Debit Mastercard Cards. Refer to Rule 3.17 for more information.

6.10 Prepaid Card Programs

6.10.6 Value Loading

In Kenya, the Rule on this subject is modified as follows.

- Value loads of winnings, unspent chips, or other value usable for gambling to a consumer Card is permitted provided the Activity is not prohibited by applicable law or regulation.
- Value loads of winnings, unspent chips, or other value usable for gambling to a commercial Card or Maestro Card is not permitted.
- Value loads of winnings, unspent chips, or other value usable for gambling to a consumer prepaid Card (excluding anonymous prepaid Cards) is permitted provided that:
  - Value loads of winnings, unspent chips, or other value usable for gambling to consumer prepaid Cards is not prohibited by applicable law or regulation; and
  - The Customer complies with the requirements set forth in Rule 6.10.

In Angola, Botswana, Comoros, Democratic Republic of the Congo, Djibouti, Eritrea, Ethiopia, Ghana, Gambia, Lesotho, Liberia, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Seychelles, Sierra Leone, Somalia, South Sudan, Swaziland, Tanzania, Uganda, Zambia, and Zimbabwe, the Rule on this subject is modified as follows.

- Value loads of winnings, unspent chips, or other value usable for gambling to a consumer Card is permitted provided the Activity is not prohibited by applicable law or regulation.
- Value loads of winnings, unspent chips, or other value usable for gambling to a commercial Card, prepaid Card, or Maestro Card is not permitted.

Chapter 16 United States Region

This chapter contains Rules pertaining to Activity conducted in the United States Region.

Applicability of Rules

The Rules in this United States Region chapter are variances and additions to the "global" Rules that apply in the United States Region. Refer to Appendix A for the United States Region geographic listing.

Definitions

Solely within the U.S. Region, the following terms have the meanings set forth below:

Acquiring Activity Fee

A fee assessed by the Corporation in connection with a "Change of Control," as such term is defined in Rule 1.12 of Chapter 16, "United States Region," of an Acquirer or the acquiring business of a Customer.

Debit, Debit Mastercard Card, Debit Card

Any Mastercard Card or Program issued in the U.S. Region by a Region Customer that when presented for payment in the United States, accesses, debits, holds, or settles funds from a consumer's demand deposit or asset account less than fourteen days after the date of the purchase.

"Debit" includes any consumer signature debit, stored value, prepaid, payroll, electronic benefit transfer, and deferred debit Card or Program. "Debit" does not include any Card or Program that accesses, debits, holds, or settles funds from the user's demand deposit or asset account fourteen or more days after the date of the purchase.

Debit Payment Network

A network, other than any network owned and operated by or that is a corporate affiliate of the Corporation, that provides access to Maestro Accounts issued in the U.S. Region at POS Terminals located in the U.S. Region through the use of payment cards and uses a common service mark to identify such POS Terminals and payment cards.

Designee

An entity, including but not limited to a Third Party Processor or a Merchant, that has been authorized by the Corporation to connect directly to the Interchange System for purposes of Maestro Transaction processing.

Mastercard Affiliate

A financial institution that is eligible and approved to be a Customer that participates indirectly in Mastercard Activity through the Sponsorship of a Mastercard Principal, an Association, or a Type I TPP utilizing the Mastercard Principal's, Association's, or Type I TPP's assigned ICAs and BINs/IINs, but which must be Sponsored by a Mastercard Principal or Association to participate in Mastercard Acquirer Activity; and as such, may not Sponsor any other Mastercard Customer.

Other Mastercard Card

Any Mastercard Card or Program issued in the U.S. Region by a Region Customer that is not defined as "debit" or "Debit Mastercard Card."

Sponsor

The relationship described in the Standards between a Principal, Association, or Type I TPP and an Affiliate that engages in Activity indirectly through the Principal, Association, or Type I TPP. In such event, the Principal, Association, or Type I TPP is the Sponsor of the Affiliate and the Affiliate is Sponsored by the Principal, Association, or Type I TPP.

Sponsorship

The relationship between a Principal, Association, or Type I TPP that Sponsors an Affiliate and that Affiliate.

TPP Acquiring Fee

A fee assessed by the Corporation in connection with a "Change of Control," as such term is defined in Rule 7.2.2 of this chapter, of a TPP.

1.9 Participation in Activity(ies) and Digital Activity

In the U.S. Region, the Rule on this subject is modified as follows.

A Mastercard Affiliate that is Sponsored by a Type I TPP may not also participate in Mastercard Activity as a Mastercard Principal or Association.

1.12 Change of Control of Customer or Portfolio

In the U.S. Region, the Rule on this subject is replaced in its entirety with the following.

1.12.1 Change of Control of Issuer or Issuing Program

In the event that an Issuer will undergo a change of Control, as the term "Control" is defined in the Definitions section of this manual, the Issuer must notify the Corporation in writing of such changes at least 90 days prior to the effective date thereof.

The Issuer must promptly provide the Corporation any information requested by the Corporation relating to such an event or proposed event and the Corporation may:

1. Suspend or impose conditions on any License granted to the Issuer or both.
2. Amend the rights or obligations or both of the Issuer.
3. Terminate the Licenses of any Issuer that:
   a. transfers or attempts to transfer Control of the Issuer to an entity that is not a Customer;
   b. merges into or is consolidated with an entity that is not a Customer,

c. sells all or substantially all of its assets;
d. sells all or substantially all of its Issuer Portfolios;
e. experiences a change in Control or Ownership; or
f. transfers or assigns, or attempts to transfer or assign, its Participation.

1.12.2 Change of Control of Acquirer or Acquiring Program

In the event that an Acquirer or the acquiring business of a Customer that is both an Issuer and an Acquirer will undergo a "Change of Control," as such term is defined herein, the Acquirer must notify the Corporation in writing of such changes at least 90 days prior to the effective date thereof.

The Acquirer must promptly provide the Corporation any information requested by the Corporation relating to such an event or proposed event and the Corporation may:

1. Suspend or impose conditions on any License granted to the Acquirer or both.
2. Amend rights or obligations or both of the Acquirer.
3. Terminate the Licenses of the Acquirer.
4. Assess an Acquiring Activity Fee. The Acquiring Activity Fee will be determined based on one or more factors which shall include, but not be limited to:
   a. The Transaction volume acquired annually by the Acquirer; or
   b. Any other factors that could significantly impact the integrity of the Mastercard system.

For purposes of this Rule, a "Change of Control" shall mean an Acquirer or the acquiring business of a Customer that is both an Issuer and an Acquirer:

1. Merges with another entity, where such other entity is the surviving entity;
2. Undergoes a transfer involving 10 percent or more of any class of its voting securities (including any options, warrants, or convertible securities that convert into voting securities) or ownership interest;
3. Undergoes a change in ownership of 10 percent or more of outstanding shares;
4. Transfers 10 percent or more of its assets, in each case in a single transaction, or a series of related transactions;
5. Undergoes a change in ownership of a "controlling interest";
6. Undergoes a change which results in a third party having the power to exercise, directly or indirectly, a controlling influence over its management or policies based on the totality of facts and circumstances;
7. Sells, transfers or closes down a specified division or line of its business which is related to or is in connection with the Corporation's business;
8. Offers all or a portion of the company to the public in an initial public offering; or
9. Undergoes a financial restructuring giving effective control to bondholders.

3.1 Obligation to Issue Mastercard Cards

In the U.S. Region, the Rule on this subject is modified as follows.

1. Any Customer that does not issue or have outstanding any cards of a competing card program within the U.S. Region is not obligated to issue Mastercard Cards to customers in the U.S. Region before it may acquire Mastercard POS Transactions from Merchants located in the U.S. Region.
2. A Customer that is Licensed to acquire Mastercard POS Transactions in the United States that extends its Area of Use to acquire Mastercard POS Transactions in Puerto Rico is not required to issue Mastercard Cards in Puerto Rico if its acquiring Activity in Puerto Rico is limited to only the Transactions of Merchants located in Puerto Rico that are also located and have headquarters in the United States, and with whom the Customer has an existing acquiring relationship in the United States.

3.3 Transaction Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

A Type I TPP that Sponsors a Mastercard Affiliate for the purpose of Issuer Activity must ensure that each Mastercard Transaction of such Affiliates that arises in connection with such Issuer Activity is a Processed Transaction.

3.7 Integrity of Brand and Network

In the U.S. Region, the Rule on this subject is modified as follows.

Pursuant to this Rule, with respect to any potentially illegal Internet gambling Transaction or any potentially illegal Internet gambling PTA Transaction, the Issuer of the Card or the Originating Institution must either employ a method of systemic Transaction or PTA Transaction blocking or decline all such Transaction authorization requests or reject such PTA Transaction on an individual basis.

An Internet gambling Transaction that may be potentially illegal when involving a U.S. Region Cardholder is any Transaction that the Acquirer has identified in the authorization request message as both:

1. A gambling Transaction, by the use of MCC 7995 or MCC 9406 in DE 18 (Merchant Type), and
2. An e-commerce Transaction, by the use of a value of 6 (electronic commerce Transaction) in DE 61 (Point of Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator).

An Internet gambling PTA Transaction that may be potentially illegal when involving a U.S. Region Account Holder is any PTA Transaction that the Originating Institution has identified in the transaction request as both:

1. A gambling PTA Transaction, by the use of MCC 7995 or MCC 9406 in DE 18 (Merchant Type), or similar coding, as may be applicable to a specific PTA Program, and
2. An e-commerce PTA Transaction, by the use of a value of 6 (electronic commerce Transaction) in DE 61 (Point of Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator), or similar coding, as may be applicable to a specific PTA Program.

An Issuer may approve, on an individual basis, any Internet gambling Transaction authorization request and a Receiving Customer may approve, on an individual basis, any PTA Transaction request, as applicable, arising from a U.S. Region Merchant and identified with MCC 7801 (Internet Gambling) or MCC 7802 (Government Licensed Horse/Dog Racing) that involves a U.S. Region Cardholder or Account Holder. In using MCC 7801, or MCC 7802, the Acquirer or Originating Institution asserts that the Transaction or PTA Transaction involves gambling activity related to horse racing, dog racing, non-sports intrastate Internet gambling, or sports intrastate Internet gambling that is deemed by the Acquirer or Originating Institution to be legal in the U.S. Region and indemnifies the Corporation in connection with all such gambling activity. Such indemnity applies regardless of the Acquirer's or the Merchant's or the Originating Institution's compliance with the Corporation's *Internet Gambling Policy* or the Standards.

5.1 The Merchant and ATM Owner Agreements

5.1.2 Required Merchant Agreement Terms

In the U.S. Region, the Rule on this subject is modified as follows.

A Merchant Agreement for Mastercard Card acceptance must provide the Merchant with the option, and the applicable Merchant discount rate for each option, to elect to accept Debit Mastercard Cards only, Other Mastercard Cards only, or both Debit Mastercard Cards and Other Mastercard Cards. With respect to any contract existing on or before 1 January 2004, under which a Merchant accepts Mastercard Cards, a Merchant may choose to stop accepting Debit Mastercard Cards or Other Mastercard Cards by providing no less than 30 days' advance written notice to its Acquirer.

A Merchant Agreement newly effective or renewed after 11 June 2014 must include a separate or distinct fee disclosure (a "Fee Disclosure").

The Fee Disclosure must clearly and conspicuously detail the methodology by which each Merchant fee (a "Fee") is calculated. As used herein, a "Fee" means any charge by an Acquirer to a Merchant related to or arising from the Merchant Agreement, including, but not limited to, a Terminal or other equipment sale charge, lease or rental; transaction processing charges; authorization, clearing and/or settlement charges; the pass-through of any Acquirer obligation to a third party; and any Merchant Agreement termination charge.

The method used to calculate each Fee listed in the Fee Disclosure, including any conditions, terms or contingencies that are or could be applicable to the Fee, must be clearly explained in plain terms. By way of example, terms that may appear in a Merchant Agreement and must be explained include, but are not limited to:

- Merchant discount rate;

- Pass-through;
- Interchange plus mark-up;
- Bundled pricing;
- Tiered rate, qualified rate, mid-qualified rate, non-qualified rate;
- Authorization; and
- Settlement or account settlement.

5.1.2.1 Gambling Merchants

In the United States Region, the Rule on this subject is modified as follows.

A Merchant may load winnings, unspent chips, or other value usable for gambling to a prepaid Card by means of a value load provided:

- It is consented to by the Issuer; and
- The load is not routed or processed through the Interchange System.

A Payment Transaction must not be processed to a prepaid Card with respect to gambling winnings, unspent chips, or other value usable for gambling.

5.4 Acquirer Obligations to Merchants

5.4.3 Provide Information

An Acquirer must provide a Merchant with which the Acquirer has a Merchant Agreement at least 30 days advance notice of any new or increased Fee arising from or related to the Merchant Agreement. Such notice must be provided separately from any regular Fee statement, bill, invoice or the like provided to a Merchant. As used herein, the term Fee has the meaning set forth in Rule 5.1.2 of these United States Region Rules.

5.8 Transaction Message Data

5.8.1 Card Acceptor Business Code (MCC) Information

In the U.S. Region, the Rule on this subject is modified as follows.

A U.S. Region Acquirer may use MCC 7801 (Internet Gambling) or MCC 7802 (Government Licensed Horse/Dog Racing) to identify Transactions arising from a U.S. Region Merchant, Submerchant, or other entity engaged in legal gambling activity involving non-sports intrastate Internet gambling, sports intrastate Internet gambling, horse racing, or dog racing if the Acquirer has first registered the Merchant, Submerchant, or other entity with the Corporation as described in section 9.4.2 of the *Security Rules and Procedures* manual.

5.11 Merchant Obligations for Card Acceptance

5.11.1 Honor All Cards

In the U.S. Region, the Rule on this subject as it applies to Mastercard Card acceptance is replaced with the following:

1. **Honor All Debit Mastercard Cards.** Merchants that choose to accept Debit Mastercard Cards must honor all valid Debit Mastercard Cards without discrimination when properly presented for payment. The Merchant must maintain a policy that does not discriminate among customers seeking to make purchases with a Debit Mastercard Card.
2. **All Other Mastercard Cards.** Merchants that choose to accept Other Mastercard Cards must honor all Other Mastercard Cards without discrimination when properly presented for payment. The Merchant must maintain a policy that does not discriminate among customers seeking to make purchases with another Card.

5.11.2 Merchant Acceptance of Mastercard Cards

Merchants that accept Mastercard Cards may choose to accept Debit Mastercard Cards only, Other Mastercard Cards only, or both Debit Mastercard Cards and Other Mastercard Cards.

Merchants that request signage for the purpose of indicating their acceptance of Debit Mastercard Cards must display such signage for a minimum of three months. The signage may be requested at www.mastercardweacceptdebit.com.

An Acquirer must provide a complete list of accurate and current BINs obtained through the Corporation that apply to Debit Mastercard Cards to its Merchants and ensure that its Merchants use the updated BIN information within six calendar days of such file being made available by the Corporation.

5.11.4 Additional Cardholder Identification

An automated fuel dispenser (MCC 5542) Merchant located in the U.S. Region and identified by the Corporation to be an Excessive Chargeback Merchant (ECM) must use the Mastercard Address Verification Service (AVS) to verify the Cardholder's ZIP code before completing a Cardholder-Activated Terminal (CAT) Level 2 Transaction. The Merchant's implementation of AVS must occur within 60 days of the initial ECM identification and continue until the Merchant is no longer identified as an ECM for three consecutive months. For information about ECM criteria, refer to the Acquirer Chargeback Monitoring Program section in the *Data Integrity Monitoring Program* manual.

5.12 Prohibited Practices

5.12.1 Discrimination

Refer to Chapter 17 for an additional provision to this Rule applicable in the U.S. Region.

6.1 Card Issuance—General Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

A Chip Card or Access Device that is newly issued or re-issued in the U.S. Region must be configured as online-only or online-preferring for both Contact Chip Transaction and Contactless Transaction processing. "Online-only" means that the Card or Access Device never approves a Transaction by means of offline authorization. "Online-preferring" means that the Card or Access Device always requests an online authorization, but may accept an offline authorization when an online connection is not available. For more information, refer to *M/Chip Requirements for Contact and Contactless*.

Transaction Alerts Service

In the U.S. Region, an Issuer in the U.S. Region must comply with the Transaction alerts service requirements set forth in Rule 6.1 of Chapter 6 by:

In addition to complying with the requirements set forth in Rule 6.1 of Chapter 6, the Issuer's support of a Transaction alerts service must include:

- Transaction alerts for Cross-border Transactions;
- Transaction alerts by Transaction type (for example, e-commerce Transactions, mail order/telephone order Transactions) or channel (for example, Card-not-present Transactions) or both; and
- The electronic delivery of Transaction alerts to Cardholders (for example, using email messages or short message service [SMS] alerts). There is no requirement regarding the speed with which the alert must be delivered, but the delivery must occur by electronic means.

In the U.S. Region, the Issuer's offering of a Transaction alerts service is required for:

- All consumer Cards except prepaid Cards that are classified as gift cards or for which the Issuer does not collect, store, or otherwise validate the consumer's identity pursuant to the *Guidelines for Anonymous Prepaid Card Programs* available on Mastercard Connect™; and
- Commercial Cards issued for use by a small business (as defined by the Corporation).

Mastercard Safety Net

In the U.S. Region, the requirement for Issuers to participate in Mastercard Safety Net or Mastercard Safety Net alerts for non-Processed Transactions does not apply.

6.1.1 Mastercard Card Issuance

In the U.S. Region, the Rule on this subject is modified as follows.

1. An Issuer must use specific and unique bank identification numbers (BINs) for Debit Mastercard Cards. Refer to Rule 3.17 for more information.
2. A Mastercard credit Card that also provides access to a debit account when a transaction occurs at a POS Terminal using PIN functionality must enable that Card to process any debit PIN POS transaction as a Maestro POS Transaction.
3. An Issuer must ensure that all of its Debit Mastercard Cards enabled for the processing of single message transactions (PIN-based and/or PIN-less) by a Competing EFT POS Network are also enabled for Transaction processing by means of the Single Message System. When Debit Mastercard Card Transactions are processed on the Single Message System, the Standards applicable to Maestro Cards and Maestro POS Transactions apply.

6.1.2 Maestro Card Issuance

In the U.S. Region, the Rule on this subject modified as follows.

A Mastercard credit Card may be enhanced with the Maestro Payment Application.

A Maestro Chip Card:

1. May support either online PIN verification only or both online PIN and offline PIN verification as the CVM for POS Transactions; and
2. Must support online PIN verification as the CVM for any Maestro Contactless Transaction that exceeds the Contactless Transaction CVM limit amount.

6.1.4 Tokenization of Accounts

In the U.S. Region, the Rule on this subject is modified as follows.

Prior to the allocation of a Mastercard Token corresponding to a debit Account issued using a Corporation-designated BIN, the Issuer must notify the Corporation of each Debit Payment Network enabled on the debit Account as a Merchant routing option.

6.1.4.1 Maestro Accounts

If Maestro is issued on a debit card other than a Debit Mastercard Card, and the other brand enabled on that debit card offers Tokenization services, the Issuer of the Maestro Account must ensure that the other Token Vault can support and respond appropriately to Token mapping and cryptography validation requests sent by the Corporation to the Token Vault with respect to single message transactions routed to the Interchange System.

6.10 Prepaid Card Programs

6.10.6 Value Loading

In the U.S. Region, the Rule on this subject is modified as follows.

Value loads arising from gambling winnings, unspent chips or other value usable for gambling, or winnings related to a lottery scheme conducted and managed by a U.S. state government body, are permitted provided that:

- Value loads of winnings are not prohibited by applicable law or regulation;
- The Card is a consumer Card;
- The Customer complies with the requirements set forth in Rule 6.10; and
- The Card is not an anonymous prepaid Card, unless the value load is USD 500 or less and represents winnings related to a lottery scheme conducted and managed by a U.S. state government body.

7.1 Service Provider Categories and Descriptions

In the U.S. Region, the "List of Services" column for "Type III", "Third Party Processor (TPP)/TPP Program Service" Category/Program Service Name is modified to add the following.

The Corporation determines, in its sole discretion, if a TPP, in addition to being a Type I TPP or a Type II TPP, is also a Type III TPP, based upon consideration of the following criteria:

1. Whether a Type I TPP performs acquiring Program Service for an Acquirer in the U.S. Region;
2. Whether the TPP owns an equity stake in the Acquirer's Mastercard Activity;
3. Whether a joint venture, business combination, strategic alliance, or other business formation is in relation to or in connection with Mastercard business. For purposes of this Rule, Mastercard business shall be defined as any activity involving the use of any Mastercard programs, services, products, systems, or other functions or of any of the Marks;
4. Whether, in the determination of the Corporation, the TPP is managing the operations of an Acquirer's Merchant acquiring program, which management may include, but not limited to, any one or more of the following activities:
   a. Receiving fees directly from the Merchant related to Mastercard Activity;
   b. Defining, or having the ability to define, the criteria employed in screening of potential Merchants or otherwise managing the merchant on-boarding process;
   c. Specifying the information to be contained in a Merchant application, the Merchant Agreement, or both; or
   d. Determining Merchant pricing; and
5. Whether the TPP is a signatory to a Merchant Agreement.

7.1.2 Third Party Processor

7.1.2.3 Type III

The Corporation determines, in its sole discretion, if a TPP, in addition to being a Type I TPP or a Type II TPP, is also a Type III TPP, based upon consideration of the following criteria:

1. Whether a Type I TPP performs acquiring Program Service for an Acquirer in the U.S. Region;
2. Whether the TPP owns an equity stake in the Acquirer's Mastercard Activity;
3. Whether a joint venture, business combination, strategic alliance, or other business formation is in relation to or in connection with Mastercard business. For purposes of this Rule, Mastercard business shall be defined as any activity involving the use of any Mastercard programs, services, products, systems, or other functions or of any of the Marks;
4. Whether, in the determination of the Corporation, the TPP is managing the operations of an Acquirer's Merchant acquiring program, which management may include, but not limited to, any one or more of the following activities:
   a. Receiving fees directly from the Merchant related to Mastercard Activity;
   b. Defining, or having the ability to define, the criteria employed in screening of potential Merchants or otherwise managing the merchant on-boarding process;
   c. Specifying the information to be contained in a Merchant application, the Merchant Agreement, or both; or
   d. Determining Merchant pricing; and
5. Whether the TPP is a signatory to a Merchant Agreement.

7.2 The Program and Performance of Program Service

7.2.2 Notification to the Corporation

In the U.S. Region, the Rule on this subject is modified as follows.

In the event a TPP performing acquiring Program Service for a U.S. Region Customer will undergo a "Change of Control," as such is defined below, the TPP must notify the Corporation in writing of such change by sending an email message to tpp_registration@mastercard.com at least 90 days prior to the effective date thereof. The TPP must promptly provide the Corporation any information requested by the Corporation relating to such an event or proposed event. The Corporation will, in writing, either:

1. Reaffirm the TPP's registration status; or
2. Reaffirm the TPP's registration status and establish additional conditions to the registration, including the assessment of a TPP Acquiring Activity Fee.

The TPP Acquiring Activity Fee will be determined based on one or more of the following factors, which shall include, but not be limited to:

1. Transaction volume processed annually by the TPP;
2. The number of Customers for which the TPP performs Program Service; or
3. Any other factors relating to the TPP's performance of Program Service that could significantly impact the integrity of the Mastercard system.

Alternatively, the Corporation may, in its sole discretion, terminate or suspend the TPP's registration.

For purposes of this Rule, a Change of Control shall mean the TPP:

1. Merges with another entity, where such other entity is the surviving entity;
2. Undergoes a transfer involving 10 percent or more of any class of its voting securities (including any options, warrants, or convertible securities that convert into voting securities) or ownership interest;
3. Undergoes a change in ownership of 10 percent or more of outstanding shares;
4. Transfers 10 percent or more of its assets, in each case in a single transaction, or a series of related transactions;
5. Undergoes a change in ownership of a "controlling interest";
6. Undergoes a change which results in a third party having the power to exercise, directly or indirectly, a controlling influence over the management or policies of the TPP based on the totality of facts and circumstances;
7. Sells, transfers, or closes down a specified division or line of its business which is related to or is in connection with the Corporation's business;
8. Offers all or a portion of the company to the public in an initial public offering; or
9. Undergoes a financial restructuring giving effective control to bondholders.

In the event that the TPP fails to provide the written notice set forth above, the Corporation may promptly take either or both of the following actions:

1. Suspend the TPP's registration; or
2. Terminate the TPP's registration upon written notice from the Corporation. Such termination is effective upon delivery, or inability to deliver after a reasonable attempt to do so, of written or actual notice by the Corporation to the TPP.

7.6 Acquiring Programs

7.6.5 Payment Facilitators and Submerchants

In the U.S. Region, the Rule on this subject is modified as follows.

An Acquirer may permit a Payment Facilitator to manage the following additional obligations on behalf of the Acquirer, and remains fully responsible for the fulfillment of each to the extent that the Payment Facilitator fails to do so.

- Include a separate or distinct Fee disclosure in the agreement with the Submerchant, as set forth in (and as the term "Fee" is defined in) Rule 5.1.2 of these United States Region Rules.
- Provide a Submerchant with which the Payment Facilitator has a Submerchant Agreement at least 30 days advance notice of any new or increased Fee arising from or related to the Submerchant Agreement. Such notice must be provided separately from any regular Fee statement, bill, invoice or the like provided to a Submerchant.

7.6.7 Staged Digital Wallet Operator Requirements

In the U.S. Region, a provision of the Rule on this subject is modified as follows:

G. MCC 6540 must not be used for a funding stage Transaction if such funds may subsequently be used for the purchase of any products or services for which the Acquirer must register the entity conducting the sale as described in Chapter 9 of the *Security Rules and Procedures*; in such event, the MCC that best describes the nature of the purchase must be used, and the funds must be segregated and made available for use by the consumer solely for the designated purpose.

7.8 Payment Facilitator Obligations

7.8.1 Submerchant Agreement

7.8.1.1 Required Submerchant Agreement Terms

In the U.S. Region, the Rule on this subject is modified as follows.

Each Submerchant Agreement that is newly effective or renewed after 11 June 2014 must include a separate or distinct fee disclosure (a "Fee Disclosure").

The Fee Disclosure must clearly and conspicuously detail the methodology by which each Submerchant fee (a "Fee") is calculated. As used herein, a "Fee" means any charge by a Payment Facilitator to a Submerchant related to or arising from the Submerchant agreement, including, but not limited to, a Terminal or other equipment sale charge, lease or rental; transaction processing charges; authorization, clearing and/or settlement charges; the pass-through of any Acquirer obligation to a third party; and any Submerchant agreement termination charge.

The method used to calculate each Fee listed in the Fee Disclosure, including any conditions, terms or contingencies that are or could be applicable to the Fee, must be clearly explained in plain terms. By way of example, terms that may appear in a Submerchant agreement and must be explained include, but are not limited to:

- Merchant discount rate;
- Pass-through;
- Interchange plus mark-up;
- Bundled pricing;
- Tiered rate, qualified rate, mid-qualified rate, non-qualified rate;
- Authorization; and
- Settlement or account settlement.

7.8.2 Obligations as Sponsor of Submerchants

In the U.S. Region, the Rule on this subject is modified as follows.

A Payment Facilitator must provide each of its Submerchants with at least 30 days advance notice of any new or increased Fee arising from or related to the Submerchant agreement. Such notice must be provided separately from any regular Fee statement, bill, invoice or the like

provided to a Submerchant. As used herein, the term Fee has the meaning set forth in Rule 7.8.1.1 of these United States Region Rules.

7.9 Type I TPP Obligations

In the U.S. Region, the Rule on this subject is as follows: The Issuer must ensure that such Issuer's Type I TPP satisfies all of the obligations set forth in this Rule.

1. In addition to engaging in TPP Program Service, a Type I TPP in the U.S. Region may Sponsor an Affiliate to engage in Mastercard and/or Maestro issuing Activity. A Type I TPP that Sponsors an Affiliate for such purpose must comply with (i) all Standards applicable to a Type I TPP; (ii) subject to Rule 8.7, all Standards applicable to a Principal Issuer; and (iii) such additional or alternative Standards and/or other requirements that the Corporation may determine to be necessary or appropriate from time to time.
2. Notwithstanding Rule 7.1 or Rule 7.3, a TPP registered as a Type I TPP for Mastercard Activity and/or Maestro Activity pursuant to Rule 7.9 may participate in Settlement as agent for a U.S. Region Customer subject to (a) through (f) below. As used in this Rule, "Settlement" and "participation in Settlement" have the meanings set forth in Chapter 1 of the *Settlement Manual*, and a "Settled-For Customer" means a U.S. Region Customer for which a Type I TPP participates in Settlement to any extent.
    a. For so long as the Type I TPP is participating in Settlement, the Type I TPP agrees to comply with all Standards applicable to Settlement and participation in Settlement and such additional or alternative Standards and/or other requirements including, by way of example and not limitation, credit criteria and collateral requirements, as the Corporation may at any time determine to be necessary or appropriate.
    b. The Corporation has no obligation to pay or reimburse, nor has any liability for any funds owed to, the Type I TPP by any Settled-For Customer with respect to any of the Settled-For Customer's Activities or any other Settled-For Customer obligation.
    c. Should the Type I TPP advance funds on behalf of a Settled- For Customer to the Corporation, such advance is deemed a loan by the Type I TPP to the Settled-For Customer and the Type I TPP bears all risk of loss without recourse of any nature to the Corporation.
    d. Unless otherwise set forth in the Standards or by a written agreement to which the Corporation is a party:
        i. The Corporation at any time may draw on Settlement funds held by a Type I TPP to satisfy any obligation arising pursuant to the Standards of any Settled-For Customer and regardless of whether any of such funds are commingled with any other funds;
        ii. The Type I TPP acknowledges and agrees that 1) the Type I TPP's participation in Settlement is issuing and/or acquiring Activity; 2) the Type I TPP is an "Indemnifying Customer" as such term is defined and used in Rule 2.3, with respect to the Type I TPP's participation in Settlement; and 3) the Type I TPP and each of the Type I TPP's Settled-For Customers are jointly and severally liable for any failure by the Type I TPP or by the Type I TPP's Settled-For Customer to comply with the Standards pertaining to Settlement and such additional or alternative Standards and/or other

requirements pertaining to Settlement that the Corporation may determine to be necessary or appropriate from time to time and at any time;

iii. In the event the Corporation draws on funds held by a Type I TPP to satisfy an obligation arising pursuant to the Standards of a Settled-For Customer, the Corporation has no obligation to reimburse the Type I TPP or such Settled-For Customer any such funds; and

iv. The Corporation has the same rights (including, without limitation, rights of set off, offset, and recoupment) with respect to Settlement funds held by a Type I TPP that the Corporation has with respect to Settlement funds held by a Customer.

e. (i) During the first week of each calendar quarter and (ii) upon request by the Corporation, within two business days of such request, the Type I TPP must provide to the Corporation in writing a list of all Settled-For Customers. With respect to each Settled-For Customer listed, the Type I TPP must provide 1) the ICA assigned to the Customer by the Corporation for use in Settlement; 2) the bank, account number and beneficiary/ owner of the account used for Settlement of the Settled-For Customer's obligations; 3) average daily Settlement volume in USD for the calendar quarter immediately preceding the current calendar quarter; and 4) the amount of any collateral and/or prepayment the Settled-For Customer has provided to the Type I TPP.

f. The Type I TPP must promptly, and in any event within two business days, provide the Corporation written notice of 1) any Customer which has now become a Settled-For Customer of the Type I TPP; 2) the termination of the Type I TPP's participation in Settlement for a Settled-For Customer or 3) any change in the bank, account number or beneficiary/owner of the account used for Settlement of a Settled-For Customer's obligations.

7.10 Registration Requirements for Service Providers

7.10.2 Registration Requirements for Type I TPPs

In the U.S. Region, the Rule on this subject is modified as follows.

In addition to TPPs that the Corporation designates to be prospective Type I TPPs, a TPP or other entity in the U.S. Region may become a Type I TPP if such TPP or other entity:

1. Is registered by the Corporation as a Type I TPP; and
2. Agrees to comply with all Standards applicable to Type I TPPs and to Principals and any additional requirements that the Corporation may deem necessary or appropriate from time to time; and
3. Provides evidence satisfactory to the Corporation that it is in compliance with Mastercard Anti-Money Laundering and Sanctions Requirements; and
4. Pays applicable fees.

7.10.3 Registration Requirements for Type III TPPs

Any Type I TPP or Type II TPP that meets one or more of the criteria set forth in Rule 7.1.2.3 of this chapter must apply to be registered by the Corporation as a Type III TPP, and the Corporation will determine, in the Corporation's discretion, if the TPP is a Type III TPP.

After registration by the Corporation of a Type III TPP, and on an annual basis, the applicable fee is charged by the Corporation directly to the Type III TPP. The renewal or continuation of a Type III TPP's registration as a TPP is at the sole discretion of the Corporation.

8.6 Settlement Liability for Debit Licensees

A debit Licensee is granted a License limited to the issuance of Debit Mastercard Cards.

A principal debit Licensee is not responsible for the Debit Mastercard Card Program obligations of any affiliate debit Licensee that it Sponsors if such an affiliate debit Licensee becomes unable or unwilling to discharge its settlement obligations.

8.7 Settlement Liability for Type I TPPs that Sponsor Affiliates

Unless otherwise provided in the Standards, a Type I TPP is not responsible for the Issuer Activity settlement obligations of an Affiliate that the Type I TPP Sponsors should such an Affiliate be unable or unwilling to discharge its Issuer Activity settlement obligations.

The Corporation assumes no liability for any settlement failure dispute that arises between a Type I TPP and an Affiliate Sponsored by such Type I TPP.

8.10 Risk of Loss

In the U.S. Region, the Rule on this subject applies with respect to affiliate debit Licensees in the same manner as it applies to Customers.

Chapter 17 Additional U.S. Region and U.S. Territory Rules

This chapter contains Rules pertaining to Activity conducted in the U.S. Region or a U.S. Territory.

Applicability of Rules

The Rules in this section are variances and additions to the "global" Rules that apply in the United States (U.S.) Region and in American Samoa, Guam, Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands (herein, "the U.S. Territories").

These Rules apply in addition to those set forth in the Asia/Pacific Region chapter, with respect to Customers located in American Samoa, Guam, and Northern Mariana Islands; the Latin America and the Caribbean Region chapter, with respect to Customers located in Puerto Rico and the U.S. Virgin Islands; and the United States Region chapter, with respect to U.S. Region Customers.

2.2 Conduct of Activity and Digital Activity

2.2.5 Mastercard Acquirers

An Acquirer of Mastercard POS Transactions must not prohibit a Merchant from requesting or encouraging a consumer to use a payment card with an acceptance brand other than Mastercard or other form of payment or a Mastercard Card of a different product type (for example, traditional cards, premium cards, or rewards cards) than the Mastercard Card the consumer initially presents, or otherwise prohibit its Merchant from engaging in actions consistent with Rule 5.11.1 of this chapter.

3.3 Transaction Requirements

For the avoidance of doubt, the Rule on this subject does not inhibit a Merchant's ability to direct the routing of a transaction conducted in the U.S. Region or a U.S. Territory with a debit Card that is issued in the U.S. Region or a U.S. Territory to any debit payment network enabled on the Card.

4.1 Right to Use the Marks

4.1.1 Protection and Registration of the Marks

The Rule on this subject, as it pertains to debit Cards issued in the U.S. Region or a U.S. Territory, is modified as follows.

No use of a Mark may be made on or in connection with any card, device or other application associated with a payment service that the Corporation deems to be competitive with any Activity except as set forth in this chapter.

4.8 Use of Marks on Maestro and Cirrus Cards

In the U.S. Region and U.S. Territories, the Rule on this subject is modified as follows.

The Maestro Brand Mark may be placed on a debit card in combination with other local/regional/international POS debit marks and/or local/international ATM marks. In the event that a debit card has an international POS debit mark on the card front, and the card has a Maestro Payment Application:

1. If any other POS debit mark appears on the card back, the Maestro Brand Mark must be displayed on the card back; or
2. If no other POS debit mark appears on the card back, the Maestro Brand Mark is not required to appear on the card back.

A card must not include any visible indication communicating that acceptance or use of the Maestro Brand Mark or the Maestro Payment Application is limited, geographically or otherwise.

The provision of the Rule on this subject that prohibits a Customer from placing any other Competing EFT POS Network debit marks on its participating Cards does not apply to Cards issued in the U.S. Region or a U.S. Territory.

4.9 Use of Marks on Mastercard Cards

In the U.S. Region and U.S. Territories, the Rule on this subject is modified as follows.

A competing or other debit point-of-sale marks may appear on a debit Card as set forth in the *Card Design Standards* or as otherwise agreed to by the Corporation.

5.12 Prohibited Practices

5.12.1 Discrimination

In the U.S. Region and U.S. Territories, the Rule on this subject is replaced with the following.

A Merchant may request or encourage a customer to use a payment card with an acceptance brand other than Mastercard or other form of payment or a Mastercard Card of a different type (for example, traditional cards, premium cards, or rewards cards) than the Mastercard Card the consumer initially presents. Except where prohibited by law, it may do so by methods that include, but are not limited to:

1. Offering the customer 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 customer uses a particular payment card with an acceptance brand other than Mastercard or other particular form of payment;
2. Offering the customer 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 customer, who initially presents a Card, uses instead another payment card or another form of payment;

3. Expressing a preference for the use of a particular payment card or form of payment;
4. Promoting the use of a particular general purpose payment card with an acceptance brand other than Mastercard or the use of a particular form or forms of payment through posted information, through the size, prominence, or sequencing of payment choices, or through other communications to customers (provided that the Merchant otherwise will abide by the Standards relating to the display of the Marks including, but not limited to, the Mastercard Acceptance Mark); or
5. Communicating to customers the reasonably estimated or actual costs incurred by the Merchant when a customer uses particular payment cards or forms of payment or the relative costs of using different general purpose payment cards or forms of payment.

Notwithstanding the foregoing, a Merchant located in the U.S. Region may not offer a discount or other benefit to a Cardholder if the Cardholder uses a particular Issuer's Card at the Point of Interaction (POI), unless the discount or other benefit is available for all other Cards of the same product type or is accessed 1) after the Transaction has been completed (for example, a credit on the billing statement or a rebate); or 2) at the time of or after the Transaction and is effected by a separate instrument and not by the Card (for example, a coupon or a voucher). A Merchant must not promote at the POI a discount or other benefit for use of a particular Issuer's Card.

5.12.2 Charges to Cardholders

In the U.S. Region and U.S. Territories, the Rule on this subject is modified as follows, with respect to Mastercard Credit Card Transactions, as the term Mastercard Credit Card Transaction is defined herein. For all other Transactions, the global Rule applies.

Definitions

Solely for the purposes of Rule 5.12.2 in this "Additional U.S. Region and U.S. Territory Rules" chapter, the following terms have the meanings set forth below:

1. "Cardholder" means the authorized user of a Mastercard Credit Card.
2. "Competitive Credit Card Brand" includes any brand of Credit Card or electronic credit payment form of a nationally accepted payment network other than Mastercard, specifically including without limitation Visa, American Express, Discover, and PayPal.
3. "Competitive Credit Card Brand Cost of Acceptance" is a Merchant's average Merchant Discount Rate applicable to transactions on a Competitive Credit Card Brand at the Merchant for the preceding one or twelve months, at the Merchant's option.
4. "Credit Card" means a card or other device that may be used to defer payment of debt or incur debt and defer its payment.
5. "Independent Consideration" means material value a Merchant receives specifically in exchange for the Merchant's agreement to waive or otherwise restrict its right to Surcharge transactions on a Competitive Credit Card Brand.
6. "Mastercard Credit Card" means a Credit Card bearing the Mastercard brand.

7. "Mastercard Credit Card Transaction" means a Transaction in which a Mastercard Credit Card is presented for payment and that is performed in accordance with the Standards.
8. The "Maximum Surcharge Cap" shall be no less than the product of 1.8 times the sum of the system-wide average effective U.S. domestic Mastercard Credit Card interchange rate plus average network fees (defined to include network set fees to Acquirers or Merchants associated with the processing of a Transaction or with the acceptance of the network's brand) as published from time to time.
9. "Merchant Discount Rate" is the fee, expressed as a percentage of the total transaction amount that a Merchant pays to its Acquirer or Service Provider for transacting on a Credit Card brand. For purposes of Brand-level and Product-level Surcharging, irrespective of whether the identified fees and costs are paid using the merchant discount or by check, withholding, offset, or otherwise, the Merchant Discount Rate shall include:
    a. The interchange rate,
    b. Network set fees associated with the processing of a transaction;
    c. Network set fees associated with the acceptance of the network's brand;
    d. The Acquirer set processing fees associated with the processing of a transaction; and
    e. Any other services for which the Acquirer is paid using the mechanism of the per transaction merchant discount fee.
    Other than the fees listed in (a) through (d) above, the Merchant Discount Rate excludes any fees (such as the cost of rental of point-of-sale terminal equipment) that are invoiced separately or not paid using the mechanism of the per-transaction merchant discount fee.
10. "Surcharge" means any fee charged by the Merchant for use of a Card. As set forth in this Rule 5.12.2, a Merchant located in the U.S. Region or a U.S. Territory may only require a Mastercard Credit Card Cardholder to pay a Surcharge by choosing to apply either of the following Surcharge methods:

    1. Brand-level Surcharge—The application of the same Surcharge to all Mastercard Credit Card Transactions regardless of the Issuer.
    2. Product-level Surcharge—The application of the same Surcharge to all Mastercard Credit Card Transactions of the same product type regardless of the Issuer.

5.12.2.1 Brand-level Surcharging

Definitions

Solely for purposes of this Rule 5.12.2.1, the following terms have the meanings set forth below:

1. "After accounting for any discounts or rebates offered by the Merchant at the Point of Interaction (POI)" means that the amount of the Surcharge for a Mastercard Credit Card or a Competitive Credit Card Brand is to include the amount of any discount or rebate that is applied to that card or brand at the POI but which is not equally applied to all Mastercard Credit Card Transactions.
2. "Mastercard Credit Card Cost of Acceptance" is:
    a. A percentage of the Mastercard Credit Card Transaction amount calculated based upon the average effective interchange rate plus the average of all fees imposed by the network upon Acquirers or Merchants as applicable to Mastercard Credit Card

Transactions at the Merchant for the preceding one or twelve months, at the Merchant's option, or

b. If a Merchant cannot determine its Mastercard Credit Card Cost of Acceptance, then the Merchant may use the Mastercard Credit Card Cost of Acceptance for the Merchant's merchant category as published from time to time on the Mastercard public website.

3. "Mastercard Surcharge Cap" is the average Merchant Discount Rate applicable to Mastercard Credit Card Transactions at the Merchant for the preceding one or twelve months, at the Merchant's option.

The following requirements apply to a Merchant that chooses to impose a Surcharge at the brand level:

1. The same Surcharge must apply to all Mastercard Credit Card Transactions after accounting for any discounts or rebates offered by the Merchant on Mastercard Credit Card Transactions at the POI. A Merchant may choose to Surcharge all face-to-face and/or non–face-to-face Mastercard Credit Card Transactions.
2. The Surcharge assessed on a Mastercard Credit Card Transaction may not exceed the lesser of:
   a. The Merchant's Mastercard Surcharge Cap, or
   b. The Maximum Surcharge Cap, as published by Mastercard from time to time
3. The Merchant must comply with the Surcharge disclosure requirements set forth in Rule 5.12.2.3 below.
4. If a Merchant's ability to Surcharge a Competitive Credit Card Brand that the Merchant accepts, in either a face-to-face or non–face-to-face environment, is limited by that Competitive Credit Card Brand in any manner other than by prohibiting a Surcharge greater than the Competitive Credit Card Brand's Cost of Acceptance, then the Merchant may Surcharge Mastercard Credit Card Transactions in accordance with (1) through (3) above pursuant to either:
   a. The same terms under which the Competitive Credit Card Brand permits a Merchant to Surcharge transactions of the Competitive Credit Card Brand in a face-to-face or non–face-to-face environment, or
   b. The same terms under which the Merchant actually Surcharges transactions of the Competitive Credit Card Brand, in a face-to-face or non–face-to-face environment, after accounting for any discounts or rebates offered by the Merchant at the POI to the Competitive Credit Card Brand Cards.
5. The requirements outlined in (4) above are not applicable if:
   a. The Competitive Credit Card Brand does not prohibit or effectively prohibit surcharging Credit Cards and the Competitive Credit Card Brand Cost of Acceptance to the Merchant is less than the Mastercard Credit Card Cost of Acceptance; or
   b. The Competitive Credit Card Brand prohibits or effectively prohibits the surcharging of Credit Cards and the Merchant Surcharges the Competitive Credit Card Brand in an amount at least equal to the lesser of:
      i. The Competitive Credit Card Brand Cost of Acceptance; or

ii. The amount of the Surcharge imposed on the Mastercard Credit Card Transaction to be Surcharged; or

c. The Merchant has entered into an agreement with the Competitive Credit Card Brand which waives or limits the Merchant's right to Surcharge transactions on that Competitive Credit Card Brand and the agreement:
   i. Is not indefinite but is for a fixed duration;
   ii. Is unique to the Merchant, not a standard agreement generally offered by the Competitive Credit Card Brand to multiple Merchants;
   iii. Is not a condition to the Merchant's acceptance of the Competitive Credit Card Brand, thus the Merchant must have the ability to accept the Competitive Credit Card Brand for payment if the agreement were not in place;
   iv. Is in exchange for Independent Consideration; and
   v. Contains a price under which the Merchant may accept Competitive Credit Card Brand transactions and surcharge those transactions up to the Merchant's Merchant Discount Rate for the Competitive Credit Card Brand after accounting for applicable discounts or rebates offered by the Merchant at the POI.

5.12.2.2 Product-level Surcharging

Definitions

Solely for purposes of this Rule 5.12.2.2, the following terms have the meanings set forth below:

1. "After accounting for any discounts or rebates offered by the Merchant at the POI" means that the amount of the Surcharge for Mastercard Credit Cards of the same product type or a Competitive Credit Card Product is to include the amount of any discount or rebate that is applied to that card or product at the POI but which is not equally applied to all Mastercard Credit Card Transactions of the same product type.
2. "Competitive Credit Card Product" includes any product within a brand of Credit Card or electronic credit payment form of a nationally accepted payment network other than Mastercard, specifically including without limitation Visa, American Express, Discover, and PayPal.
3. "Competitive Credit Card Product Cost of Acceptance" means 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 twelve months, at the Merchant's option.
4. "Debit Card Cost of Acceptance" means the amount of the cap for debit transactions established by the Board of Governors of the Federal Reserve System pursuant to 15 U.S. C. § 1690-2 and its implementing regulations or, if the Board of Governors discontinues establishing a cap for debit transactions, the merchant's average effective Merchant Discount Rate for all PIN-based debit transactions for the preceding twelve months.
5. "Mastercard Credit Card Product Cost of Acceptance" means:
   a. The average effective interchange rate plus the average of all fees imposed by the network upon Acquirers or Merchants, expressed as a percentage of the Transaction amount, applicable to Mastercard Credit Card Transactions of a product type at the Merchant for the preceding one or twelve months, at the merchant's option; or

   b. If a Merchant cannot determine its Mastercard Credit Card Product Cost of Acceptance, then the Merchant may use the Mastercard Credit Card Product Cost of Acceptance for its Merchant category as published by Mastercard on the Mastercard public website.

6. The "Mastercard Credit Surcharge Cap" for a product type is the average effective Merchant Discount Rate applicable to Mastercard Credit Card Transactions of that product type at the Merchant for the preceding twelve 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 Mastercard Credit Card Transactions may be deemed a proxy for this amount.

The following requirements apply to a Merchant that chooses to impose a Surcharge at the product level:

1. The same Surcharge must apply to all Mastercard Credit Card Transactions of the same product type (for example, Standard Mastercard, World Mastercard, World Elite Mastercard) after accounting for any discounts or rebates offered by the Merchant at the POI. A Merchant may choose to Surcharge all face-to-face and/or non–face-to-face Mastercard Credit Card Transactions of the same product type.
2. The Surcharge assessed on a Mastercard Credit Card Transaction may not exceed the lesser of:
   a. The Merchant's Mastercard Credit Surcharge Cap for that product type minus the Debit Card Cost of Acceptance, or
   b. The Maximum Surcharge Cap, as published by Mastercard from time to time.
3. The Merchant must comply with the surcharge disclosure requirements set forth in Rule 5.11.2.3 below.
4. If a Merchant's ability to Surcharge a Competitive Credit Card Brand that the Merchant accepts, in either a face-to-face or non–face-to-face environment, is limited by that Competitive Credit Card Brand in any manner other than by prohibiting a surcharge greater than the Competitive Credit Card Brand's Cost of Acceptance, then the Merchant may Surcharge Mastercard Credit Card Transactions in accordance with (1) through (3) above pursuant to either:
   a. The same terms under which the Competitive Credit Card Brand permits a Merchant to surcharge transactions of the Competitive Credit Card Brand in a face-to-face or non–face-to-face environment, or
   b. The same terms under which the Merchant actually surcharges transactions of the Competitive Credit Card Brand, in a face-to-face or non-face-to-face environment, after accounting for any discounts or rebates offered by the Merchant at the POI on the Competitive Credit Card Brand.
5. The requirements outlined in (4) above are not applicable if:
   a. The Competitive Credit Card Brand does not prohibit or effectively prohibit surcharging Credit Cards and the Competitive Credit Card Product Cost of Acceptance to the Merchant is less than the Mastercard Credit Card Product Cost of Acceptance, or
   b. The Competitive Credit Card Brand prohibits or effectively prohibits the surcharging of Credit Cards and the Merchant surcharges the Competitive Credit Card Brand in an amount at least equal to the lesser of:
      i. The Competitive Credit Card Brand Cost of Acceptance, or

ii. The amount of the Surcharge imposed on the Mastercard Credit Card Transaction to be Surcharged, or

c. The Merchant has entered into an agreement with a Competitive Credit Card Brand which waives or limits the Merchant's right to surcharge transactions on that Competitive Credit Card Brand and the agreement:
   i. Is not indefinite but is for a fixed duration;
   ii. Is unique to the Merchant, not a standard agreement generally offered by the Competitive Credit Card Brand to multiple Merchants;
   iii. Is not a condition to the Merchant's acceptance of the Competitive Credit Card Brand, the Merchant must have the ability to accept the Competitive Credit Card Brand for payment if the agreement were not in place;
   iv. Is in exchange for Independent Consideration; and
   v. Contains a price under which the Merchant may accept Competitive Credit Card Brand transactions and surcharge those transactions up to the Merchant's Merchant Discount Rate for the Competitive Credit Card Brand after accounting for applicable discounts or rebates offered by the Merchant at the POI.

5.12.2.3 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 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.

5.12.2.4 Merchant Notification and Acquirer Registration

A Merchant that chooses to impose a Surcharge must provide Mastercard and its Acquirer with no less than 30 days' advance written notice that the Merchant intends to impose a Surcharge on Mastercard Credit Card Transactions at either the brand level or product level.

For information about how to notify Mastercard, see https://www.mastercard.us/en-us/surcharge-disclosure-webform.html. The Acquirer must register the identity of the Merchant with Mastercard within 10 days of receipt of the Merchant's notification.

5.12.2.5 Transaction Requirements

The Acquirer of a Merchant that chooses to apply either a Brand-level Surcharge or a Product-level Surcharge to Mastercard Credit Card Transactions must offer to the Merchant the ability to electronically submit to the Acquirer any such Surcharge amount separately (in the defined surcharge field) from the Transaction amount in the authorization and clearing message.

The Transaction amount will include the purchase amount plus the surcharge amount. If the Merchant separately submits the Surcharge amount applied to a Transaction electronically, the Acquirer must transmit the Surcharge amount in DE 28 (Amount, Transaction Fee) of the authorization request message and in DE 54 (Amounts, Additional), subfield 5 (Additional Amount, Amount) of the clearing message. DE 54 also must contain a value of 42 (Amount, Surcharge) in subfield 2 (Additional Amount, Amount Type).

For the avoidance of doubt, a Merchant is not prohibited from applying a Brand-level or Product-level Surcharge if the Acquirer has not enabled the Merchant to electronically submit the Surcharge amount separately from the Transaction amount as set forth in this Rule 5.12.2.5. A Merchant that applies a Brand-level or Product-level Surcharge must disclose the Surcharge amount on the TID as set forth set forth in Rule 5.12.2.3.

In the event that a Merchant provides a full or partial refund of a purchase Transaction that included a Brand-Level or Product-Level Surcharge, the refund Transaction must include the full or prorated Brand-Level or Product-Level Surcharge amount.

5.12.3 Minimum/Maximum Transaction Amount Prohibited

In the U.S. Region and U.S. Territories, the Rule on this subject is modified as follows.

A Merchant may set a **minimum Transaction amount** to accept a Mastercard Card that provides access to a credit account, under the following conditions:

1. The minimum Transaction amount does not differentiate between Issuers; and
2. The minimum Transaction amount does not differentiate between Mastercard and another acceptance brand; and
3. The minimum Transaction amount does not exceed USD 10 (or any higher amount established by the Federal Reserve by regulation).

A Merchant may set a **maximum Transaction amount** to accept a Mastercard Card that provides access to a credit account, under the following conditions:

1. The Merchant is:
   a. A department, agency or instrumentality of the U.S. Government;
   b. A corporation owned or controlled by the U.S. Government; or
   c. A Merchant whose primary business is reflected by one of the following MCCs:
      - MCC 8220—Colleges, Universities, Professional Schools, Junior Colleges; or
      - MCC 8244—Schools, Business and Secretarial; or
      - MCC 8249—Schools, Trade and Vocational; and
2. The maximum Transaction amount does not differentiate between Issuers; and
3. The maximum Transaction amount does not differentiate between Mastercard and another acceptance brand.

5.12.8 Disparagement

A Merchant must not disparage the Corporation or any of the Corporation's products, programs, services, networks, or systems.

Chapter 18 Value-Added Services

This chapter contains Rules that apply to Customers that elect to participate in Value-Added Services.

18.1 Introduction/Applicability

Value-Added Services Rules, including the defined terms set forth herein, are part of the Mastercard Rules and Standards, but are applicable only to Value-Added Services provided by Mastercard or a Mastercard Supplier. These Value-Added Services Rules shall apply to those Value-Added Services in which a Customer elects to participate on or after the initial publication date of these Value-Added Services Rules. Value-Added Services Rules shall not apply to Mastercard's core network authorization, clearing, and settlement services, a Customer's use of Brand Marks, a Customer's compliance with Card manufacturing Standards, and any other Activity performed by the Customer pursuant to a License or requirements related thereto.

18.2 Definitions

Any capitalized term not defined in this Rule shall have the meaning set forth within the body of the Value-Added Services Rules and/or the Mastercard Rules or Documentation, each as defined below and as applicable. For the avoidance of doubt, the Definitions in this chapter are solely applicable to the procurement and use of the Value-Added Services.

"Affiliate" means, with respect to any Person, any other Person that, directly or indirectly, through one or more intermediaries, Controls, is Controlled by, or is under common Control with such Person.

"Applicable Data Protection Law" means all applicable law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation or rule (each as amended and replaced from time to time) which relates to the protection of Data Subjects with regards to the Processing of Personal Data to which the Parties are subject, including but not limited to the EU Data Protection Law; the California Consumer Privacy Act; the U.S. Gramm-Leach-Bliley Act; Brazil Data Protection Law; the South Africa Protection of Personal Information Act; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws governing the portability and/or cross-border transfer of Personal Data; and all other similar international, federal, state, provincial, and local requirements; each as applicable.

"Confidential Information" has the meaning set forth in Rule 18.5 of these Value-Added Services Rules.

"Control" means the power to direct or control the management and policies of a Person through the ownership of voting securities, by contract or otherwise.

"Customer" means any entity that procures directly from Mastercard a Value-Added Service, including but not limited to "Customer" as that term is defined elsewhere in the Mastercard Rules.

"Customer Intellectual Property" means (i) of a Customer's computer software, websites, programs, documentation, manuals, processes, procedures, systems, and sales materials; (ii)

Customer Marks; and (iii) any and all improvements, enhancements, modifications, alterations, or derivative works of or to any of the items mentioned in (i) and (ii) herein.

"Customer Marks" means any Marks created by or on behalf of a Customer.

"Customer Materials" means any data, files, materials or information (if any) provided by the Customer to Mastercard or a Mastercard Supplier in connection with the Value-Added Services.

"Data Subject" means a Cardholder, or other natural person whose Personal Data is processed in the context of the Value-Added Services.

"Deliverables" means all reports, data, materials, documents, or other deliverables provided by Mastercard to a Customer in connection with the Value-Added Services.

"Documentation" means program guides, implementation guides, manuals, announcements, pricing bulletins and other pricing arrangements, the Enrollment Form, release notes, reference guides, specifications, or other documents relating to the Value-Added Services (as defined below) provided or made available by Mastercard to the Customer.

"Enrollment Form" means an executed form or statement of work by Mastercard and a Customer, reflecting the procurement by the Customer of one or more Value-Added Services.

"Intellectual Property" means Customer Intellectual Property or Mastercard Intellectual Property, as applicable.

"Intellectual Property Rights" means any and all now or hereafter known tangible and intangible (i) rights associated with works of authorship throughout the world, including copyrights or works of copyright, moral rights, and mask-works; (ii) Marks and similar rights; (iii) trade secret rights; (iv) patents, designs, algorithms, and other industrial property rights; (v) all other intellectual and industrial property rights of every kind and nature throughout the world and however designated (including domain names, logos, "rental" rights, and rights to remuneration), whether arising by operation of law, contract, license, or otherwise; and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions, or reissues thereof currently or hereafter in force (including any derivative rights in any of the foregoing).

"License" has the meaning set forth in the Definitions appendix of the Mastercard Rules.

"Look and Feel" means the elements of graphics, design, organization, presentation, layout, user interface, navigation, trade dress, and stylistic convention (including the digital implementations thereof) developed by a Party or its service providers and unique to a Party.

"Marks" means trademarks and service marks (whether registered or at common law), trade names, business names, logos, sounds, animations, haptics, visual depictions, symbols, and Internet domain names, or any abbreviation or contraction thereof.

"Mastercard" means Mastercard International Incorporated and/or the Mastercard entity providing the Value-Added Services, as set forth in the Enrollment Form or other Documentation.

"Mastercard Binding Corporate Rules" or **"Mastercard BCRs"** means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available on Mastercard's public facing website.

"Mastercard Intellectual Property" means (i) the Value-Added Services and Deliverables (excluding any Customer Materials, Customer Marks, or Personal Data embedded therein), and any and all software, websites, programs, and other applications provided or made available by Mastercard in connection with any of the foregoing, and the user experience and Look and Feel of any of the foregoing; (ii) all Documentation, computer software, processes, procedures, systems, sales materials, technical materials, checklists, and any other documentation issued or made available by Mastercard; (iii) the Mastercard Marks; and (iv) any and all improvements, enhancements, modifications, alterations, or derivative works of or to any of the items mentioned in (i), (ii), and (iii) herein.

"Mastercard Marks" means any Marks created by or on behalf of Mastercard.

"Mastercard Rules and Standards" means the Mastercard Rules and Standards, including this chapter and any successor versions thereof.

"Mastercard Supplier" means a third party engaged by Mastercard to provide all or part of the Value-Added Services or make available or provide all or part of the Value-Added Services.

"Net Fees" means either (i) in the case of Value-Added Services provided by Mastercard that are not a component of a Card program, the fees for the Value-Added Services set forth in the Documentation specific to such Value-Added Services or bundle of Value-Added Services; or (ii) in the case of Value-Added Services that are provided by Mastercard as a component of a Card program, the 'services fee' or Card assessment fee, as applicable, plus any other fees specific to such Value-Added Services or bundle of Value-Added Services, as set forth in the Documentation, and in each of clauses (i) and (ii), less any rebates, incentives (including in-kind contributions provided by Mastercard attributed to such Value-Added Services), or other discounts provided by Mastercard.

"Person" means and includes any individual, partnership, joint venture, corporation, company, bank, trust, unincorporated organization, government, or any department, agency, or instrumentality thereof.

"Personal Data" means any information relating to an identified or identifiable individual, including contact information, demographic information, passport number, Social Security number or other national identification number, bank account information, Primary Account Number and authentication information (e.g. identification codes, passwords)

"Personnel" means the employees, agents, and contractors of Mastercard and/or a Mastercard Supplier.

"Processing of Personal Data" (or **"Processing/Process"**) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction including any operation defined as "Processing" under applicable Privacy and Data Protection Law.

"Sub-Processor" means the entity engaged by the Customer or any further sub-contractor to Process Personal Data on behalf of and under the instructions of Mastercard.

"Territory" means the countries set forth on the Enrollment Form or Documentation.

"Value-Added Service" means feature, service, functionality product or technology provided by Mastercard or identified in Mastercard Documentation as governed by this chapter of the *Mastercard Rules*. For the avoidance of doubt, Value-Added Services do not include Mastercard services pertaining to Activity (as defined in the *Mastercard Rules*), the licensing of any Brand Marks, Card manufacturing Standards, or Interchange System services (e.g., core network authorization, clearing, and settlement).

"Value-Added Services Rules" mean the Rules set forth in this chapter.

18.3 Responsibilities of a Party

18.3.1 Mastercard Responsibilities

Mastercard and/or a Mastercard Supplier will provide or make available the Value-Added Services to a Customer in accordance with the Enrollment Form and/or Documentation and these Value-Added Services Rules. Personnel that perform or provide the Value-Added Services shall (i) have the requisite skill and physical resources necessary to provide the Value-Added Services; and (ii) perform the Value-Added Services in a competent, professional, and workmanlike manner in accordance with industry standards.

18.3.1.1 Information Security

Mastercard will complete an annual SSAE 18 (or its then current equivalent) review and provide to the Customer a copy of any reports that Mastercard receives related to compliance with the SSAE 18, upon written request from the Customer, once per year. The SSAE 18 report shall be a "Type II" report (as specified in the SSAE 18). Any information provided by Mastercard in connection with the SSAE 18 shall be deemed to be Confidential Information under these Value-Added Services Rules.

18.3.1.2 Business Continuity and Disaster Recovery

If applicable for a Value-Added Service, Mastercard will maintain a formal business continuity program ("Business Continuity Program" or "BCP") that will include plans for emergency response and management, business recovery, and disaster recovery. These plans will be made available for review to the Customer upon request at a mutually agreeable time and location. BCP documentation will not be available for distribution, as it contains Mastercard Confidential Information. Mastercard agrees to annually test its BCP and provide confirmation of exercises, upon request. Mastercard will also provide information to the Customer required for the Customer's development of BCP plans that work in concert with the Mastercard BCP, if requested. Mastercard represents and warrants that disaster recovery plans shall, at a minimum, address (i) the backup and restoration of operating systems and applications supporting processing at an alternate facility; (ii) the backup and recovery of critical data received from the Customer; and (iii) the operational recovery of the Value-Added Services within the defined recovery time objective, unless otherwise communicated. In the event that Mastercard facilities supporting the Value-Added Services are inoperable, Mastercard shall treat the Customer no less favorably than Mastercard treats its other Customer(s).

18.3.2 Customer Responsibilities

A Customer shall (i) obtain all consents, information, and materials necessary from third parties and local authorities(other than Mastercard Suppliers) for Mastercard to provide the Value-Added Services; (ii) use the Value-Added Services, and access, use, and/or operate the Value-Added Services and Deliverables, solely in accordance with these Value-Added Services Rules and the Documentation; (iii) be solely responsible for its use of the Value-Added Services, and access, use, and/or operation of the Deliverables, as well as its implementation of or reliance on any advice or recommendations provided in connection with the Value-Added Services and Deliverables; (iv) provide Mastercard, in a timely fashion, with all information requested by Mastercard in connection with or related to the performance of the Value-Added Services; and (v) fulfill its obligations and responsibilities as otherwise stated in the Documentation.

18.4 Fees, Invoices, and Taxes

18.4.1 Fees and Invoices

The fees due from a Customer are set out in the Documentation, and will be invoiced by Mastercard and paid by the Customer using the Mastercard Consolidated Billing System (MCBS) or as otherwise stated in the Documentation.

18.4.2 Taxes

All payments made, consideration provided, and the value of services rendered by Mastercard under these Value-Added Services Rules and the Documentation shall be exclusive of any applicable sales tax, withholding tax, use tax, goods and services tax, value-added tax (VAT), stamp duties, business occupation tax, or any other applicable tax or charge of a similar nature (collectively, **"Taxes"**). Unless otherwise set forth in the Documentation or required by applicable law, the Customer has the sole obligation to collect, report, and remit any Taxes.

Mastercard shall provide an invoice to the Customer compliant with the applicable sales tax or VAT legislation. To the extent that a Customer is required by applicable law to deduct an amount on account of any withholding tax imposed or levied by the federal, state, or local government or any other applicable taxing authority, the amount paid by the Customer for the Value-Added Services hereunder shall be increased such that the amount received by Mastercard is equal to the payment which would have been due from the Customer if no deduction for withholding tax had been required. Where applicable, it is the Customer's responsibility to furnish Mastercard with valid certificates or other evidence supporting applicable exemptions from sales, use, or excise taxes. Each Party shall be responsible for its own income taxes, personal property taxes, payroll taxes, and similar taxes.

18.5 Confidentiality

18.5.1 Confidential Information

"Confidential Information" means all information disclosed by one Party (**"Discloser"**) to the other Party (**"Recipient"**) (in writing, orally, or in any other form) that is identified at the time of disclosure as confidential or should have reasonably been known by the Recipient to be confidential (including, without limitation, trade secrets and unpublished patent applications, and, for Mastercard, the Mastercard Intellectual Property or any data and information contained therein), together with any documents prepared by the Recipient that contain, otherwise reflect, or, in whole or in part, are generated from such disclosed information. Confidential Information does not include information or material that (i) is now, or hereafter becomes, through no act or failure to act on the part of the Recipient, publicly known or available; (ii) is or was known by the Recipient at or before the time such information or material was received from the Discloser, as evidenced by the Recipient's tangible (including written or electronic) records; (iii) is furnished to the Recipient by a third party that is not under an obligation of confidentiality to the Discloser with respect to such information or material; or (iv) is independently developed by the Recipient or on behalf of the Recipient without any use of the Discloser's Confidential Information.

18.5.1.1 Protection and Use

For the period during which a Customer elects to participate in the Value-Added Service and for a period of three (3) years thereafter, each Party shall take all reasonable measures to protect the confidentiality of the other Party's Confidential Information in a manner that is at least as protective as the measures that it uses to maintain the confidentiality of its own Confidential Information, but not less than a reasonable standard. Each Recipient shall hold the other Party's Confidential Information in strict confidence and shall not disclose, copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of such information, or give or disclose such information to third parties, or use such information for any purpose other than as necessary to fulfill its obligations or exercise its rights under these Value-Added Services Rules and the Documentation. Notwithstanding the foregoing, the Recipient may disclose the Discloser's Confidential Information (i) to employees, consultants, and subcontractors that have a need to know such information, provided that the Recipient shall advise each such employee and consultant of their obligations to keep such information confidential; and (ii) to the extent that the Recipient is legally compelled to disclose such Confidential Information pursuant to subpoena or the order of any governmental authority; provided that, where possible and permitted by applicable law, the Recipient shall give advance notice of such compelled disclosure to the Discloser, and shall cooperate with the Discloser in connection with efforts to prevent or limit the scope of such disclosure and/or use of the Confidential Information.

18.5.1.2 Return of Confidential Information

Except as otherwise stated in the Documentation, upon termination of these Value-Added Services Rules, or such earlier time as the Discloser requests, the Recipient shall return to the Discloser, or, at the Discloser's request, securely destroy all Confidential Information in the

Recipient's possession. Notwithstanding the foregoing, the Recipient is not obligated to destroy Confidential Information (i) commingled with other information of the Recipient if it would be a substantial administrative burden to excise such Confidential Information; (ii) contained in an archived computer system backup made in accordance with the Recipient's security or disaster recovery procedures; or (iii) required to be retained pursuant to applicable law, regulatory requirements, or post-termination obligations as stated in the Documentation, provided in each case that such Confidential Information remains subject to the obligations of confidentiality in this Rule 18.5 until the eventual destruction.

18.6 Privacy and Data Protection

Mastercard and each Customer must comply with Applicable Data Protection Law when Processing Personal Data in the context of the Value-Added Service.

18.6.1 Processing of Personal Data for Purposes of Value-Added Service

A Customer is the organization responsible for complying with the Applicable Data Protection Law in respect of the collection, use and disclosure of Personal Data, including the transfer of Personal Data outside the country of origin, for the purposes of the Value-Added Service, and Mastercard acts as an entity that Processes Personal Data on behalf of the Customer for these purposes.

For such activities, Mastercard will only undertake Processing of Personal Data in accordance with (1) the Customer's instructions where they are compliance with Applicable Data Protection Law and (2) the Standards, and will comply with appropriate organizational, physical and security measures, as applicable to Mastercard under the Applicable Data Protection Law.

NOTE: Modifications to this Rule appear in Rule 18.6.8, "Europe Region Variances and Additions", Rule 18.6.9, "Brazil Variances and Additions" and Rule 18.6.10, "Mainland China Variances and Additions".

18.6.2 Data Subject Notice and Consent

A Customer must ensure that Data Subjects are provided with appropriate notice and, if necessary, have given proper consent in accordance with the Applicable Data Protection Law so that Personal Data relating to them may be collected, used, disclosed, transferred (including any overseas transfers) or otherwise Processed by the applicable Customer and Mastercard for the purposes set forth in the Standards.

NOTE: Modifications to this Rule appear in Rule 18.6.8, "Europe Region Variances and Additions", Rule 18.6.9, "Brazil Variances and Additions" and Rule 18.6.10, "Mainland China Variances and Additions".

18.6.3 Data Subject Rights

In accordance with the Applicable Data Protection Law, a Customer must develop and implement appropriate procedures for handling requests by Data Subjects for access to,

correction, deletion and/or other applicable rights of the Data Subjects in relation to Personal Data Processed by the applicable Customer or Mastercard.

The Customer is responsible for responding to such requests. Mastercard will cooperate with the Customer in responding to such requests and will provide access to Personal Data held by Mastercard where required by the Applicable Data Protection Law.

If a request as described above is made by a Data Subject directly to Mastercard, a Customer must cooperate with Mastercard in promptly responding to the request.

NOTE: Modifications to this Rule appear in Rule 18.6.8, "Europe Region Variances and Additions", Rule 18.6.9, "Brazil Variances and Additions" and Rule 18.6.10, "Mainland China Variances and Additions".

18.6.4 Personal Data Accuracy and Data Minimization

Customers must take reasonable steps to ensure that Personal Data which the Customer provides to Mastercard is:

- accurate, complete, and current;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed; and
- kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed, unless a longer retention is required or allowed under applicable law.

18.6.5 Data Transfers

The Customer authorizes Mastercard to Process Personal Data in accordance with Applicable Data Protection Law in locations outside of the country where the Customer is located (including the United States of America) and/or where the Data Subjects are located (including the United States of America) for the purposes set forth in the Standards.

18.6.6 Sub-Processing

Each Customer authorizes Mastercard to use internal and external Sub-Processors for the purposes of carrying out the Value-Added Service. Mastercard will require its Sub-Processors, using a written agreement, to comply with Applicable Data Protection Law and with the same obligations as are imposed on Mastercard by the Standards and, where applicable, by Mastercard Binding Corporate Rules.

NOTE: Modifications to this Rule appear in Rule 18.6.8, "Europe Region Variances and Additions", Rule 18.6.9, "Brazil Variances and Additions" and Rule 18.6.10, "Mainland China Variances and Additions".

18.6.7 Returning or Destroying Personal Data

A Customer must destroy, delete, identify, or return (where applicable) any Personal Data it Processes, holds, retains or stores where either upon termination of the Processing services, the Data Subject requests deletion or return of the Personal Data, or the Personal Data is no longer

necessary for the purposes set out in the Standards, unless applicable law prevents the Customer from returning or destroying all or part of the Personal Data or requires storage of the Personal Data. Where the Personal Data is retained, Mastercard and/or the Customer will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore.

18.6.8 Europe Region Variances and Additions

A Customer that is subject to Applicable Data Protection Law in the Europe Region must comply with both 18.6 and this Rule 18.6.8, which applies to Processing of Personal Data subject to EU Data Protection Law.

As used in this Rule, the following terms have the meanings as described below.

"**Controller**" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

"**Disclosure Request**" means any request by a Government Agency for access to, or disclosure of, Personal Data for law enforcement, national security regulatory reporting or other purposes.

"**EU Data Protection Law**" means the EU General Data Protection Regulation 2016/679 and the e-Privacy Directive 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them in any country in the European Economic Area ("EEA"); the UK GDPR and Data Protection Act 2018; and the Monaco Data Protection Act (as amended and replaced from time to time); the Swiss Federal Data Protection Act (the "FADP"); and any legislation and/or regulation which amends, replaces, re-enacts or consolidates any of them.

"**Government Agency**" means any competent public or quasi-public authority (including without limitation regulators, local government authorities, law enforcement authorities and national security agencies) of any jurisdiction that may request disclosure of Personal Data Processed in connection with the Services.

"**Mastercard Binding Corporate Rules**" or "**Mastercard BCRs**" means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities, available on Mastercard's public facing website.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or other unauthorized Processing of Personal Data transmitted, stored, or otherwise Processed.

"**Processor**" means the entity which Processes Personal Data on behalf of a Controller.

"**Sensitive Data**" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any future revision of EU Data Protection Law.

"**Standard Contractual Clauses**" or "**SCCs**" means

With respect to Personal Data to which the GDPR applies, the standard contractual clauses for the transfer of Personal Data to Third Countries pursuant to the GDPR, adopted by the

European Commission under Commission Implementing Decision (EU) 2021/914, and not including any clauses marked as optional ("EU Standard Contractual Clauses" or "EU SCCs").

With respect to Personal Data to which the FADP applies, the EU SCCs, provided that any references in the clauses to the GDPR shall refer to the FADP.

With respect to Personal Data to which the FADP applies, the EU SCCs, provided that any references in the clauses to the GDPR shall refer to the FADP.

- the details of Mastercard and Customer in table 1 of the UK Addendum shall be as set out in Annex 1 of Section 18.6.8.12 (with no requirement for signature);
- for the purposes of table 2 of the UK Addendum, the first option is selected and the "Approved EU SCCs" are those incorporated as per the paragraph above; and
- the appendix information listed in table 3 of the UK Addendum is set out in Annex 1 and Annex 2 of Section 18.6.8.12.

"**Third Country**" means a country where the laws applicable to Personal Data do not offer the same level of protection for such Personal Data as the laws applicable in the country where the Customer's Data Subject is located.

"**UK Data Protection Law**" means (i) the Data Protection Act 2018; (ii) the GDPR as amended by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 ('UK GDPR') as relevant; and (iii) the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) as transposed into UK national law.

18.6.8.1 Processing of Personal Data for Purposes of Value-Added Service

In the Europe Region, Rule 18.6.1 is modified to include the following.

A Customer is a Controller with regard to the Processing of Personal Data for the purposes of carrying out Value-Added Services, and Mastercard acts as a Processor for these purposes.

Each Customer acknowledges that Mastercard may Process, as a Controller, Personal Data for the purposes of accounting, auditing and billing; fraud, financial crime and risk management; defense against claims, litigation and other liabilities; arbitration and other decisions made for dispute resolution; product development and improvement; internal research, reporting and analysis; anonymization of data to develop data analytics products; and compliance with legal obligations. Mastercard represents and warrants that it will Process Personal Data for these purposes in compliance with EU Data Protection Law and the Standards and in line with the description of the Processing activities set forth in the Mastercard BCRs.

To the extent that it acts as a Processor, Mastercard will: (1) cooperate with Customers in their role as Controllers to fulfill their data protection compliance obligations in accordance with EU Data Protection Law; (2) only undertake Processing of Personal Data in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in the Standards, the Mastercard BCRs, or as otherwise agreed in writing; and (3) comply with obligations equivalent to those imposed on the Customers as Controllers by the applicable provisions of EU Data Protection Law, including those applicable to Processors and data transfers.

Mastercard will notify the Customer when local laws prevent Mastercard (1) from complying with the Customer's instructions (except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), and (2) from fulfilling its obligations under the Standards or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by the Standards or the Mastercard BCRs.

18.6.8.2 Mastercard BCRs

Mastercard will abide by the Mastercard BCRs when the Processing of Personal Data is or was subject to EU Data Protection Law.

18.6.8.3 Data Subject Notice and Consent

In the Europe Region, Rule 18.6.2 is modified to include the following.

A Customer must ensure that the Processing of Personal Data for the purposes provided in Rule 18.6.1 relies on a valid legal ground under EU Data Protection Law, including obtaining Data Subjects' proper consent where required or appropriate under EU Data Protection Law.

Customers must ensure that Data Subjects receive appropriate notice, in a timely manner: (1) with at the minimum all of the elements required under EU Data Protection Law, (2) about the existence of Processors located outside of the EEA or the relevant country where relevant; and (3) where required or appropriate, about the existence of the Mastercard BCRs, including about Data Subjects' right to enforce the Mastercard BCRs as third-party beneficiaries (by referring to the public version of the Mastercard BCRs).

18.6.8.4 Data Subject Rights

In the Europe Region, Rule 18.6.3 is modified to include the following.

A Customer must develop and implement appropriate procedures for handling Data Subjects' requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing of Personal Data, (f) objection, and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them.

To the extent that Mastercard acts as a Processor, Mastercard will assist the Customer in complying with its obligation to respond to such requests, including by providing access to Personal Data maintained by Mastercard.

18.6.8.5 Accountability

Taking into account the nature, scope, context, and purposes of Processing of Personal Data, as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, Mastercard and the Customers must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that Processing of Personal Data is performed in accordance with the Standards, and EU Data Protection Law, including, as applicable, by appointing a data protection officer, maintaining records of Processing of Personal Data, complying with the principles of data protection by design and by default, performing data protection impact assessments, appropriate documentation on international

transfers of Personal Data and conducting prior consultations with supervisory authorities. Mastercard will cooperate with and assist the Customers in fulfilling their own obligations under EU Data Protection Law.

18.6.8.6 International Data Transfers

Each Customer authorizes Mastercard to transfer the Personal Data Processed subject to EU Data Protection Law outside of the Europe Region, and in particular into the United States Region and India, in accordance with the Mastercard BCRs or with any other lawful data transfer mechanism that provides an adequate level of protection under EU Data Protection Law.

To the extent that Mastercard makes any transfer of Personal Data Processed in connection with the Services to an entity in a Third Country outside the scope of the Mastercard BCRs (for which another lawful data transfer mechanism is required to provide an adequate level of protection under EU Data Protection Law or UK Data Protection Law), Mastercard and the Customer agree to enter into and comply with the obligations set out in the SCCs, which are hereby incorporated by reference, as though such obligations were set out in full in these Standards, and with the Customer's and Mastercard's signature and dating of the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound by these Standards being deemed to be the signature and dating of the SCCs.

The EU SCCs are completed as follows: Mastercard and Customer conclude module four of the EU SCCs (processor-to-controller) of the EU SCCs.

- The "data exporter" is Mastercard; the "data importer" is the Customer;
- Clause 16 (Governing law): the clauses shall be governed by the laws of Belgium;
- The information as required by Annex I of the SCCs is as set out in Annex 1 of this section

If Mastercard's compliance with EU Data Protection Law or UK Data Protection Law applicable to international data transfers is affected by circumstances outside of Mastercard's control, including if a legal instrument for international data transfers is invalidated, amended, or replaced, then Customer and Mastercard will work together in good faith to reasonably resolve such non-compliance.

In the event Mastercard is compelled to comply with a Disclosure Request and such disclosure causes Customer to breach EU Data Protection Law or UK Data Protection Law, the Customer represents and warrants that it will not hold Mastercard liable for such disclosure. The Customer further agrees that, to the greatest extent authorized by applicable law, it will not revoke or amend its instruction to Process Personal Data unless strictly required by EU Data Protection Law. Any amendments to the Customer's instructions to Process Personal Data, such as where necessary to ensure the continued compliance with EU Data Protection Law, must be agreed by both Mastercard and Customer in writing prior to taking effect.

18.6.8.7 Sub-Processing

In the Europe Region, Rule 18.6.6 is modified to include the following.

To the extent that Mastercard acts as a Processor, the Customer gives a general authorization to Mastercard to Process and sub-Process Personal Data internal and external Sub-Processors in the context of the Services under the conditions set forth below and when sub-Processing the Processing of Personal Data in the context of the Services, Mastercard:

- Binds its internal Sub-Processors to respect Mastercard BCRs and to comply with the Customers' instructions.
- Requires its external Sub-Processors, using a written agreement, to comply with the requirements of EU Data Protection Law applicable to Processors and data transfers, with the Customers' instructions, and with the same obligations as are imposed on Mastercard by the Standards and the Mastercard BCRs, including sub-Processing and audit requirements set forth in Mastercard BCRs.
- Remains liable to the Customer for the performance of its Sub-Processors' obligations.
- Commits to provide a list of Sub-Processors to the Customer upon request.
- Will inform Customer of any addition or replacement of a Sub-Processor in a timely fashion so as to give Customer an opportunity to object to the change before the Personal Data is communicated to the new Sub-Processor.

18.6.8.8 Government Requests for Personal Data

Where Mastercard is requested to disclose Personal Data to a Government Agency that Mastercard is Processing, Mastercard will only comply with such request in accordance with the Mastercard BCRs and EU Data Protection Law. Where Mastercard is acting as a Processor, Mastercard will refer the Goverment Agency to the Customer, unless Mastercard is prohibited from doing so.

18.6.8.9 Security and Data Protection Audit

In accordance with the Standards and EU Data Protection Law, Mastercard and each Customer must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including during the transmission of the Personal Data.

In assessing the appropriate level of security, Mastercard and the Customer must take into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

Mastercard and each Customer must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and as applicable Processes Personal Data in accordance with the Customer's instructions.

Upon prior written request by the Customer, to the extent that Mastercard acts as a Processor and subject to the strictest confidentiality obligations, Mastercard will, within reasonable time, provide a Customer with: (a) a summary of the audit reports demonstrating Mastercard's compliance with EU Data Protection Law and Mastercard BCRs, after redacting any

confidential or commercially sensitive information; and (b) a confirmation that the audit has not revealed any material vulnerability in Mastercard's systems, or to the extent that any such vulnerability was detected that Mastercard has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with EU Data Protection Law and the Mastercard BCRs, or reveal some material issues, subject to the strictest confidentiality obligations, Mastercard will allow the Customer to request an audit of Mastercard's data protection compliance program by external independent auditors, which are jointly selected by Mastercard and the Customer. The external independent auditor cannot be a competitor of Mastercard, and Mastercard and the Customer will mutually agree upon the scope, timing, cost and duration of the audit. Mastercard will make available to the Customer the result of the audit of its data protection compliance program.

18.6.8.10 Personal Data Breaches

Where Mastercard acts as a Processor, Mastercard will inform the Customer, without undue delay, and no later than 48 hours after having become aware of it, of a Personal Data Breach.

Mastercard will assist the Customer in complying with its own obligations to notify a Personal Data Breach. Mastercard and each Customer must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects, and the remedial action taken.

18.6.8.11 Liability for EU Data Protection Law Violations

Where the Customer or Mastercard acts as a Controller, it is responsible for the damage caused by the Processing of Personal Data which infringes the Data Protection sections in the Standards and EU Data Protection Law.

To the extent that Mastercard acts as a Processor, it will be liable for the damage caused by Processing only where it has not complied with obligations of EU Data Protection Law specifically directed to Processors or where it has acted outside or contrary to lawful instructions of the Customer. Mastercard will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where one or more Customers and/or Mastercard are involved in the same Processing of Personal Data and where they are responsible for any damage caused by Processing of Personal Data, each may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Mastercard paid full compensation for the damage suffered, it is entitled to claim back from the Customer(s) involved in the same Processing of Personal Data that part of the compensation corresponding to their part of responsibility for the damage.

18.6.8.12 Annexes for Processing of Personal Data

Annex 1 to Section 18.6.8: Processing of Personal Data

A. List of Parties

1. Data exporter: Mastercard
   - Name and address of Mastercard as well as the name, position, and contact details for Mastercard's contact person: as stipulated in the relevant License Agreement, Services

Agreement or other enrollment form, announcement, license agreement or any other documents by which Customer is bound.

- Activities relevant to the data transferred: the Services
- Signature and date: as stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or another documents by which Customer is bound.
- Role: As set out in Section 18.6.8.1 or as stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other documents by which Customer is bound.

2. Data importer: Customer
   - Name and Address of Customer as well as the name, position, and contact details for Customer's contact person: as stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.
   - Activities relevant to the data transferred: Participating in, or benefiting from, the Services.
   - Signature and date: as stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, or license agreement by which Customer is bound by those Standards.
   - Role: As set out in Section 18.6.8.1 of those Standards or as stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other documents by which Customer is bound.

B. Description of the Transfer

Data Subjects

As stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Categories of data

Confidential Transaction Data, including PAN data, date, time and amount of Transaction or as stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Sensitive Data transferred

The Customer and Mastercard do not Process any Sensitive Data in the context of the Services unless as stipulated otherwise in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Frequency of the transfer

Continuous.

Nature of the Processing

Collection, storage, analysis, disclosure by transfer or otherwise making available.

Purposes of the transfer(s)

The transfer is made for the purposes set forth in Section 18.6.8.1 or as stipulated in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

Period for which the Personal data will be retained

Personal Data will be retained only for as long as necessary to provide the services covered under the Services.

C. Competent Supervisory Authority

The Belgian Data Protection Authority.

Annex 2 to Section 18.6.8: Technical and Organizational Measures to Ensure the Security of Data

The Customer and Mastercard will, as a minimum, implement the following types of security measures:

Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, including:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (e.g., ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Having door locking (e.g., electric door openers);
- Having security staff or janitors;
- Using Surveillance facilities, video/CCTV monitor, alarm system; and
- Securing decentralized data processing equipment and personal computers.

Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons, including:

- User identification and authentication procedures;
- ID/password security procedures (e.g., special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts; and
- Creation of one master record per user, user master data procedures, per data processing environment.

Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (e.g., profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure; and
- Deletion procedure.

Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, including:

- Tunneling
- Logging; and
- Transport security.

Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including:

- Logging and reporting systems; and
- Audit trails and documentation.

Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the instructions of the Controller, including:

- Unambiguous wording for the Controller's instructions;
- Formal commissioning (request form); and
- Criteria for selecting the Processor.

Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical), including:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);

- Uninterruptible power supply);
- Remote storage;
- Anti-virus/firewall systems; and
- Disaster recovery plan.

Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately, including:

- Separation of databases;
- Access and use restrictions on a need-to-know basis
- Segregation of functions (e,g., production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

Annex 3 to Section 18.6.8: Sub-Processing of Personal Data

List of Sub-Processors

As listed in https://techdocs.mastercard.com/bundle/m_GDPR/page/vcd1642413792117.htmlor in the relevant License Agreement, Services Agreement or other enrollment form, announcement, license agreement or any other relevant documents by which Customer is bound.

18.6.9 Brazil Variances and Additions

A Customer that is subject to Brazil Data Protection Law must comply with both Rule 18.6 and this Rule 18.6.9, which applies to the Processing of Personal Data subject to Brazil Data Protection Law.

As used in this Rule, the following terms have the meanings as described below.

"**Brazil Data Protection Law**" means any law, statute, declaration, decree, legislation, enactment, order, ordinance, directive, regulation or rule (as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which Mastercard and the Customer are subject in Brazil, including but not limited to the Brazil General Data Protection Act (Law 13.709/2018).

"**Controller**" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or other unauthorized Processing of Personal Data transmitted, stored, or otherwise Processed.

"**Processor**" means the entity that Processes Personal Data on behalf of a Controller.

"**Sensitive Data**" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as

any other type of data that will be considered to be sensitive according to Brazil Data Protection Law.

"**Sub-Processor**" means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

18.6.9.1 Processing for purposes of Value-Added Service

In Brazil, Rule 18.6.1 is modified to include the following.

A Customer is a Controller with regard to the Processing of Personal Data for the purposes of carrying out its Value-Added Services, and Mastercard acts as a Processor for these purposes.

Each Customer acknowledges that Mastercard may Process, as a Controller, Personal Data for the purposes of accounting, auditing and billing; fraud, financial crime and risk management; defense against claims, litigation and other liabilities; arbitration and other decisions relating to dispute resolution; product development and improvement; internal research, reporting and analysis; anonymization of data to develop data analytics products; and compliance with legal obligations. Mastercard represents and warrants that it will process Personal Data for these purposes in compliance with Brazil Data Protection Law and the Standards.

To the extent that it acts as a Processor, Mastercard will: (1) cooperate with Customers in their role as Controllers to fulfill their data protection compliance obligations in accordance with Brazil Data Protection Law; (2) only undertake Processing of Personal Data in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in the Standards or as otherwise agreed in writing; and (3) comply with obligations equivalent to those imposed on the Customers as Controllers by the applicable provisions of Brazil Data Protection Law, including those applicable to Processors and data transfers.

Mastercard will notify the Customer when local laws prevent Mastercard (1) from complying with the Customer's instructions (except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), and (2) from fulfilling its obligations under the Standards and have a substantial adverse effect on the guarantees provided by the Standards.

18.6.9.2 Data Subject Notice and Consent

In Brazil, Rule 18.6.2 is modified to include the following.

A Customer must ensure that the Processing of Personal Data for the purposes provided in Rule 18.6.1 relies on a valid legal ground under Brazil Data Protection Law, including obtaining Data Subjects' proper consent where required or appropriate under Brazil Protection Law.

A Customer must ensure that Data Subjects receive appropriate notice, in a timely manner: (1) with at the minimum all of the elements required under Brazil Data Protection Law, and (2) about the existence of Processors located outside of Brazil.

18.6.9.3 Data Subject Rights

In Brazil, Rule 18.6.3 is modified to include the following.

A Customer must develop and implement appropriate procedures for handling Data Subjects' requests to exercise their rights under Brazil Data Protection Law, including, as applicable, the right of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing of Personal Data, (f) objection, and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them.

To the extent that Mastercard acts as a Processor, Mastercard will assist the Customer in complying with its obligation to respond to such requests, including by providing access to Personal Data maintained by Mastercard.

18.6.9.4 Accountability

Taking into account the nature, scope, context, and purposes of Processing of Personal Data, as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, Mastercard and the Customers must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that Processing of Personal Data is performed in accordance with the Standards and Brazil Data Protection Law, including, as applicable, by appointing a data protection officer, maintaining records of Processing of Personal Data, complying with the principles of data protection by design and by default, performing data protection impact assessments, and conducting prior consultations with supervisory authorities. Mastercard will cooperate with the Customer to ensure compliance with and to assist the Customer in fulfilling their own obligations under Brazil Data Protection Law.

18.6.9.5 International Data Transfers

The Customer authorizes Mastercard to transfer the Personal Data Processed subject to Brazil Data Protection Law outside of Brazil in accordance with Brazil Data Protection Law.

18.6.9.6 Sub-Processing

In Brazil, Rule 18.6.6 is modified to include the following.

To the extent that Mastercard acts as a Processor, the Customer gives a general authorization to Mastercard to use internal and external Sub-Processors on its behalf.

Mastercard requires its Sub-Processors, using a written agreement, to comply with the requirements of Brazil Data Protection Law, with the Customers' instructions, and with the same obligations as are imposed on Mastercard by the Standards.

18.6.9.7 Disclosures of Personal Data

Where Mastercard is requested to disclose Personal Data to a law enforcement authority or state security body ("Requesting Agency") that Mastercard is Processing, the Corporation will only comply with such request in accordance with Brazil Data Protection Law. Where Mastercard is acting as a Processor, Mastercard will refer the Requesting Agency to the Customer, unless Mastercard is prohibited from doing so.

18.6.9.8 Security and Data Protection Audit

In accordance with the Standards and Brazil Data Protection Law, Mastercard and each Customer must implement and maintain a comprehensive written information security program

with appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate level of security, Mastercard and the Customer must take into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of Processing of Personal Data, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

Mastercard and each Customer must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and as applicable Processes Personal Data in accordance with the Customer's instructions.

18.6.9.9 Personal Data Breaches

Where Mastercard acts as a Processor, and where required under Brazil Data Protection Law, the Corporation will inform the Customer, without undue delay, of a Personal Data Breach.

Mastercard will assist the Customer in complying with its own obligations to notify a Personal Data Breach. Mastercard and each Customer must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects, and the remedial action taken.

18.6.9.10 Liability for Brazil Data Protection Law Violations

Where the Customer or Mastercard acts as a Controller, it is responsible for the damage caused by the Processing of Personal Data which infringes Brazil Data Protection Law or these Standards. To the extent that Mastercard acts as a Processor, it will be liable for the damage caused by Processing of Personal Data only where it has not complied with obligations of Brazil Data Protection Law specifically directed to Processors or where it has acted outside or contrary to lawful instructions of the Controller. Mastercard will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where one or more Customers and/or Mastercard are involved in the same Processing of Personal Data and where they are responsible for any damage caused by Processing of Personal Data, each may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Mastercard paid full compensation for the damage suffered, it is entitled to claim back from the Customer(s) involved in the same Processing of Personal Data that part of the compensation corresponding to their part of responsibility for the damage.

18.6.10 Mainland China Variances and Additions

A Customer that is subject to China Data Protection Law must comply with China Data Protection Law, Rule 18.6 and this Rule 18.6.10, which applies to the Processing of Personal Data subject to China Data Protection Law.

As used in this Rule, the following terms have the meanings as described below.

"Mainland China" means the mainland of the People's Republic of China, excluding the Hong Kong Special Administrative Region, the Macao Special Administrative Region and Taiwan.

"China Data Protection Law" means any law, statute, declaration, decree, legislation, enactment, order, ordinance, directive, regulation or rule (as amended and replaced from time to time) promulgated by the relevant competent authorities in Mainland China which regulates the Processing of Personal Data to which the Customer (and where applicable, Mastercard) are subject in Mainland China, including but not limited to the Personal Information Protection Law of the People's Republic of China.

"Controller" means the entity (or individual) which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or other unauthorized Processing of Personal Data transmitted, stored, or otherwise Processed.

"Processor" means the entity (or individual) which Processes Personal Data on behalf of a Controller.

"Sensitive Personal Data" means any Personal Data that is considered to be sensitive according to China Data Protection Law, including any Personal Data that, if leaked or illegally used, is likely to cause harm to a natural person's personal dignity or endanger a natural person's personal or property safety, including Personal Data revealing biometrics, religious beliefs, particular capacity, medical treatments, health, financial accounts, tracks, etc., and Personal Data of minors under the age of 14.

"Sub-Processor" means the entity (or individual) engaged by a Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the relevant Controller.

18.6.10.1 Processing of Personal Data for Purposes of Value-Added Services

In Mainland China, Rule 18.6.1 is modified to include the following.

A Customer is a Controller with regard to the Processing of Personal Data for the purposes of carrying out Value-Added Services, and Mastercard acts as a Processor for these purposes.

Each Customer acknowledges that Mastercard may Process, as a Controller, Personal Data for the purposes of accounting, auditing and billing; fraud, financial crime and risk management; defense against claims, litigation and other liabilities; arbitration and other decisions relating to dispute resolution; product development and improvement; internal research, reporting and analysis; anonymization of data to develop data analytics products; and compliance with legal obligations. Mastercard represents and warrants that it will Process Personal Data for these purposes in compliance with China Data Protection Law (where applicable) and the Standards.

To the extent that it acts as a Processor, Mastercard will: (1) cooperate with the Customer in its role as the Controller to fulfill their data protection compliance obligations in accordance with China Data Protection Law; (2) only undertake Processing of Personal Data in accordance with the Customer's instructions where they are in compliance with China Data Protection Law and the Standards and not for any other purposes or by other means than those specified in the Standards, the Customer's instructions, or as otherwise agreed in writing; and (3) adopt

appropriate organizational, physical and security measures to safeguard the security of Personal Data Processed.

18.6.10.2 Data Subject Notice and Consent

In Mainland China, Rule 18.6.2 is modified to include the following.

A Customer must ensure that the Processing of Personal Data for the purposes provided in Rule 18.6.1 is based on a valid legal ground under China Data Protection Law, including obtaining Data Subjects' proper consent (including separate consent) where required or appropriate under China Data Protection Law, so that Personal Data (including Sensitive Personal Data, if any) relating to them may be collected, used, disclosed, transferred (including any overseas transfers) or otherwise Processed by the applicable Customer and Mastercard for the purposes set forth in the Standards.

A Customer must ensure that Data Subjects are provided with appropriate notice with at the minimum all of the elements required under China Data Protection Law (including with respect to the Processing of Sensitive Personal Data and overseas transfers of Personal Data to the Mastercard entity located outside of Mainland China, including Mastercard International Incorporated in the U.S.A., and Mastercard Asia/Pacific Pte. Ltd. in Singapore and other affiliates).

18.6.10.3 Data Subject Rights

In Mainland China, Rule 18.6.3 is modified to include the following.

A Customer must develop and implement appropriate procedures for handling Data Subjects' requests to exercise their rights under China Data Protection Law, including, as applicable, the right of (a) access, (b) rectification, (c) erasure, (d) data transfer, (e) restriction of Processing of Personal Data, (f) objection, (g) requesting for explanation regarding the rules as to the Processing of Personal Data, and (h) not being subject to a decision based solely on automated processing, including profiling, which materially affects such Data Subjects' rights and interests.

To the extent that Mastercard acts as a Controller or where required by China Data Protection Law, Mastercard will also develop and implement appropriate procedures for responding to such requests from Data Subjects.

To the extent that Mastercard acts as a Processor, Mastercard will inform the Customer of requests it directly receives from Data Subjects and the Customer shall be responsible for responding to such requests from Data Subjects.

18.6.10.4 Accountability

Taking into account the nature, scope, context, means, and purposes of Processing of Personal Data, as well as the impact on the rights and interests of Data Subjects and the security risks that are presented by the Processing of Personal Data, the Customer (and where required under China Data Protection Law, Mastercard) must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that Processing of Personal Data is performed in accordance with the Standards and China Data Protection Law, including, as applicable, by appointing a data protection officer, maintaining records of Processing of Personal Data, complying with the principles of Processing established in China Data Protection Law, and performing data protection impact assessments. To the extent that Mastercard acts

as a Processor, Mastercard will cooperate with the Customer to ensure compliance with and to assist the Customer in fulfilling their own obligations under China Data Protection Law.

18.6.10.5 International Data Transfers

Each Customer authorizes Mastercard to transfer Personal Data Processed subject to China Data Protection Law outside of Mainland China, to the extent permissible under, and in accordance with, China Data Protection Law.

Each Customer acknowledges that for the purposes of carrying out Value-Added Services, the Customer may transfer Personal Data outside of Mainland China to the Mastercard entity located out of Mainland China, to the extent permissible under, and in accordance with, China Data Protection Law and the applicable contractual requirements issued by the relevant competent authorities. Notwithstanding any other provisions under the Data Protection sections in the Standards to the contrary, the clauses under the applicable contractual requirements issued by the relevant competent authorities should be incorporated into this Rule 18.6.10.5 by reference. To the extent required by China Data Protection Law, each Customer shall (a) complete self-assessment to identify and assess if any security risks may arise from or in connection with the cross-border transfer of Personal Data, and (b) pass the security assessment administered by the relevant competent authorities, in compliance with China Data Protection Law.

18.6.10.6 Sub-Processing

In Mainland China, Rule 18.6.6 is modified to include the following.

To the extent that Mastercard acts as a Processor, subject to any requirements under China Data Protection Law, the Customer gives a general authorization to Mastercard to use internal and external Sub-Processors on its behalf.

Mastercard requires its Sub-Processors, via a written agreement, to comply with the requirements of China Data Protection Law applicable to Sub-Processors, with the Customers' instructions, and with the same obligations as are imposed on Mastercard by the Standards.

18.6.10.7 Security

In accordance with the Standards and China Data Protection Law, each Customer (and where required under China Data Protection Law, Mastercard) must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate level of security, the Customer (and where required under China Data Protection Law, Mastercard) must take into account the nature, scope, context, means, and purposes of Processing of Personal Data, as well as the impact on the rights and interests of Data Subjects and the security risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed. The Customer (and where required under China Data Protection Law, Mastercard) shall also take into account the appropriate level of security in the event of a material change in (i) actual control; (ii) scope of business; or (iii) regulatory and legal environment of the residing country/region, that may impact the security of the data.

Mastercard and Customer must each take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and as applicable Processes Personal Data in accordance with the Customer's instructions.

18.6.10.8 Data Retention; Deleting Personal Data

Mastercard will retain Personal Data for no longer than is necessary for the purposes for which the Personal Data are Processed, unless a longer retention period is required or allowed under applicable law.

Upon termination of the Processing services or upon request by the Customer (to the extent that Mastercard acts as a Processor), or upon expiry of retention period (whether Mastercard acting as a Controller or a Processor), Mastercard will delete, anonymize, or return (where applicable and feasible) such Personal Data it Processes, holds, retains or stores, unless applicable law prevents Mastercard from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case Mastercard will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore).

18.6.10.9 Personal Data Breaches

Where Mastercard acts as a Processor, and where required under China Data Protection Law, Mastercard will (a) inform the Customer, without undue delay, of a Personal Data Breach; and (b) provide reasonable assistance to the Customer in complying with its own obligations in respect of a Personal Data Breach (which may include to implement emergency response plan, notify the relevant competent authorities and affected Data Subjects of the Personal Data Breach (if required), and provide a smooth channel for Data Subjects to safeguard their rights and interests concerning Personal Data).

18.6.10.10 Liability for China Data Protection Law Violations

The Customer, as a Controller, is responsible for the actual damage caused by the Processing of Personal Data which is in violation of the Data Protection sections in the Standards and China Data Protection Law.

To the extent that Mastercard acts as a Controller, it is responsible for the actual damage caused by the Processing of Personal Data which is in violation of the Data Protection sections in the Standards and China Data Protection Law (to the extent applicable).

To the extent that Mastercard acts as a Processor, it will be liable for the damage caused by the Processing of Personal Data only where it has acted intentionally or out of gross negligence in regard to non-compliance with obligations under China Data Protection Law (to the extent applicable) specifically directed to Processors or with lawful instructions of the Controller Customer.

To the maximum extent permissible by applicable law or regulation, liability as between Mastercard (whether acting as a Controller or a Processor) and the Customer is limited to actual damage suffered, and in no event shall a party be liable to the other party or any third party for any loss of profits, revenue or goodwill, costs of procurement of substitute products or services, loss of interruption of business, loss of anticipated savings, or loss of data or any

exemplary, punitive, consequential, expectancy, special, indirect or incidental damages of any kind.

To the extent that the Customer and Mastercard are held jointly and severally liable by the relevant competent authorities for any damage caused to a third party by the Processing of Personal Data, where Mastercard has paid full compensation for the damage suffered, it is entitled to claim back from the Customer involved in the same Processing of Personal Data that part of the compensation not attributable to Mastercard's intentional misconduct or gross negligence.

18.6.10.11 Applicable Law and Jurisdiction

Any clauses under these Value-Added Services Rules in relation to the Processing of Personal Data subject to China Data Protection Law (including the Rule 18.6 and the Rule 18.6.10, "Mainland China Data Processing Rules") shall be governed by and shall be construed in accordance with, the laws of Singapore.

Any dispute arising from or in connection with the Mainland China Data Processing Rules, including any question regarding its existence, validity or termination, shall first be referred to the authorized representatives of the parties for amicable settlement. Any dispute which cannot be resolved by amicable discussions within thirty (30) days of referral shall be submitted to the Presidents (or equivalent) of the respective parties or their nominees for resolution. If the parties fail to resolve such dispute through good faith negotiations, such dispute shall be referred to and finally resolved by arbitration administered by the Singapore International Arbitration Centre (the SIAC) in accordance with the Arbitration Rules of the SIAC (the SIAC Rules) for the time being in force, which rules are deemed to be incorporated by reference in this Rule 18.6.10.11. The seat of the arbitration shall be Singapore. The tribunal shall consist of one (1) arbitrator. The language of the arbitration shall be English. Nothing in this Rule 18.6.10.11 shall preclude a party from resorting to any court of competent jurisdiction for interim or interlocutory injunctive relief.

A person or entity who is not a party to the Mainland China Data Processing Rules shall have no right under the Contracts (Rights of Third Parties) Act, Chapter 53B to enforce any term of the Mainland China Data Processing Rules.

18.6.11 Data Uses

The Parties acknowledge and agree that Mastercard may Process Personal Data and Confidential Information for the following purposes:

1. To provide the Value-Added Services in accordance with the Value-Added Services Rules, and the purposes set out in the Documentation, and Enrollment Form, including processing Transactions, creation and management of profiles and accounts, accounting, auditing, billing, reconciliation, and collection activities;
2. As may be appropriate to Mastercard's Affiliates', sub-Processors, staff, accountants, auditors, or counsel;
3. As may be required or requested by any judicial process or governmental agency having or claiming jurisdiction over Mastercard or Mastercard's Affiliates;
4. For the purpose of processing and resolving chargebacks or other disputes;

5. For the purpose of managing risk exposures and protecting against or preventing actual or potential fraud, unauthorized transactions, claims, or other liability including to third parties providing these services;
6. For product development and improvement purposes, and providing products or services to customers or other third parties;
7. For the purpose of administering sweepstakes, contests, or other marketing promotions;
8. For preparing internal reports for use by Mastercard or any of Mastercard's Affiliates, staff, management, and consultants for the purposes of operating, evaluating, and managing Mastercard's business;
9. For preparing and furnishing compilations, analyses, and other reports of aggregated or anonymized information provided that such compilations, analyses, or other reports do not identify Customers and do not identify any Data Subjects whose Transactions were involved in the preparation of the compilation, analysis, or other report;
10. For the purpose of complying with applicable legal requirements; and
11. For other purposes for which consent has been provided by the Data Subject to whom the information relates.

18.6.12 Security Safeguards

Each Party shall maintain a comprehensive written information security program that includes technical, physical, and administrative/organizational safeguards designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; (iii) protect against any actual or suspected unauthorized Processing, loss, or acquisition of any Personal Data; and (iv) ensure the proper disposal of Personal Data. In addition, such program shall include regularly testing or otherwise monitoring the effectiveness of the safeguards.

18.6.13 No Waiver

Notwithstanding anything set forth in these Value-Added Services Rules, neither Party shall be in any way restricted from Processing Personal Data in accordance with the Mastercard Rules, these Value-Added Services Rules or other Documentation, or as otherwise authorized by applicable law.

18.7 Use of Marks

18.7.1 Customer Marks

Subject to the terms of this Rule 18.7, the Customer hereby grants to Mastercard, during the period during which the Customer elects to participate in the Value-Added Service, a non-exclusive, non-transferable, royalty-free license to use, reproduce, and display the Customer Marks (i) as may be necessary for Mastercard to perform its obligations under these Value-Added Services Rules; (ii) to identify the Customer as a Mastercard customer in Mastercard sales materials; and (iii) as may be otherwise stated in the applicable Documentation; provided

that Mastercard shall provide the sales materials to the Customer for its review. The Customer (x) shall use commercially reasonable efforts to approve or disapprove the use of Customer Marks in such sales materials within five (5) business days, or such alternate time period as may be stated in the Documentation; (y) shall not unreasonably withhold its approval; and (z) agrees that its approval of such sales materials in the first instance is deemed approval for all subsequent instances.

18.7.2 Mastercard Marks

The Customer shall not use any of the Mastercard Marks without Mastercard's prior written approval in each instance. Subject to this Rule 18.7.2, the applicable Mastercard Rules (including, without limitation, branding guidelines) and the applicable Documentation, Mastercard hereby grants to the Customer a non-exclusive, non-transferable, royalty-free license to use and reproduce the Mastercard Marks, during the period during which the Customer elects to participate in the Value-Added Service, solely for the purposes as stated in the applicable Documentation or as otherwise agreed upon by Mastercard in writing.

18.7.3 Rights

Each Party acknowledges the ownership right of the other Party in the Marks of such other Party and agrees that all use of the other Party's Marks shall inure to the benefit, and be on behalf of, the other Party. Each Party acknowledges that its utilization of the other Party's Marks will not create in it, nor will it represent it has, any right, title, or interest in and to such Marks, other than the licenses expressly granted herein. Each Party agrees not to do anything contesting or impairing the existing Intellectual Property Rights in the Marks of the other Party in connection with these Value-Added Services Rules.

18.8 Termination

18.8.1 Termination of the Value-Added Services

18.8.1.1 Termination by Either Party

Either Party may terminate an individual Value-Added Service under either the applicable Enrollment Form or applicable Documentation upon thirty (30) days' notice, or such notice period as otherwise stated in the Documentation for the Value-Added Service, if the other Party has breached a material obligation, representation, or warranty as stated in these Value-Added Services Rules with respect to such Value-Added Service, and fails to cure such breach within the cure period as stated in the Documentation or, if no such period is specified therein, within thirty (30) days of receiving notice of such breach. The Parties acknowledge and agree that termination of all Value-Added Services pursuant to the preceding sentence is an effective termination of the Enrollment Form or the relevant section(s) of the Documentation. Either Party may terminate the Value-Added Services promptly upon notice if the other Party (i) becomes insolvent; (ii) is declared bankrupt; (iii) is placed under receivership; (iv) makes an

assignment for the benefit of creditors; (v) commences any proceedings for the winding up of its business, dissolution, or liquidation; or (vi) ceases to pay its debts as they come due.

18.8.1.2 Termination by Mastercard

At any time, Mastercard may terminate or suspend any Value-Added Service, in its sole discretion (i) upon ninety (90) days' notice, if Mastercard discontinues the subject Value-Added Service in one or more of the countries in the Territory; (ii) effective immediately and without prior notice, if required by applicable law or the relevant governing authority, if Mastercard is required by such law or governing authority to cease providing such Value-Added Service to such Customer or in one or more countries in the Territory; or (iii) Mastercard has reason to believe that not terminating or suspending such participation would be harmful to Mastercard's goodwill or reputation, or (iv) if Mastercard has received a claim or notice alleging that such Value-Added Service infringes or violates a third party's Intellectual Property Right.

18.8.2 Effect of Termination

Termination or expiration of the Value-Added Services shall not relieve either Party of any obligation accrued through the date of termination or expiration.

18.9 Ownership, Licenses, and Restrictions on Use

18.9.1 Mastercard Ownership

Mastercard and/or its licensors own and retain all right, title, and interest in and to the Mastercard Intellectual Property and any and all Intellectual Property Rights therein. The Customer shall execute such documentation as is reasonably necessary to document and assign to Mastercard and/or its licensors any rights in any Mastercard Intellectual Property created by or for the Customer or that otherwise arise or vest in the Customer hereunder in the Mastercard Intellectual Property. No rights are granted to the Customer or any third party in the Mastercard Intellectual Property except as explicitly stated herein.

18.9.2 Customer Ownership; License to Customer Branding

The Customer and/or its licensors own and retain all right, title, and interest in and to the Customer Materials, Customer Intellectual Property, and any and all Intellectual Property Rights within any of the foregoing. The Customer hereby grants to Mastercard a non-exclusive, royalty-free, worldwide license to use and access the Customer Intellectual Property during the period during which the Customer elects to participate in the Value-Added Service solely as necessary and appropriate for Mastercard to provide the Value-Added Services. No rights are granted to Mastercard or any third party in the Customer Intellectual Property, except as explicitly set out hereunder. The Customer grants Mastercard a non-exclusive, sub-licensable right to use and reproduce Customer branding for the period during which the Customer elects to participate in the Value-Added Service, as reasonably required for Mastercard to market the Customer's involvement in the Value-Added Service, perform its obligations, and exercise its rights under this Agreement.

18.9.3 Value-Added Services License

During the period during which the Customer elects to participate in the Value-Added Service, Mastercard hereby grants to the Customer a non-exclusive, non-transferable, non-sublicensable, non-assignable, revocable license in the Territory to use, access, connect to, and display a Value-Added Service, as applicable for such Value-Added Service and pursuant to the relevant Documentation, solely in accordance with the terms of these Value-Added Services Rules.

If a Customer provides any feedback, comments or suggestions to Mastercard regarding the Mastercard Intellectual Property ("Feedback"), the Customer gives Mastercard the right to use such Feedback without restriction.

18.9.4 Deliverables

18.9.4.1 Acceptance Criteria for Deliverables

After receipt of a Deliverable relating to a customized request or order by a Customer, the Customer shall have thirty (30) days, or such shorter time as set forth in the applicable Documentation, to provide Mastercard with notice if the Deliverable does not substantially comply with the specifications set forth in such Documentation. In such event, Mastercard will re-perform the applicable Value-Added Service to bring such Deliverable in conformance with such specifications, or take such other action as stated in the applicable Documentation.

18.9.4.2 Ownership

Mastercard and/or the Mastercard Suppliers own and retain all right, title, and interest in and to (i) any underlying data and information contained in the Deliverables (except for any Customer Materials, Customer Marks, or Personal Data contained therein); (ii) all related materials employed in performing the Value-Added Services; and (iii) all ideas, concepts, general skills, know-how, processes, methodologies, and techniques resulting from or acquired or used in the course of or arising out of the performance of the Value-Added Services.

18.9.4.3 Licenses

During the period during which the Customer elects to participate in the Value-Added Service or such shorter period as may be stated in the relevant Documentation, Mastercard hereby grants to the Customer a non-exclusive, non-transferable, non-sublicensable, non-assignable, revocable license to use the Deliverables in the Territory, solely in accordance with the terms of these Value-Added Services Rules. The Customer hereby grants to Mastercard a royalty-free, worldwide license and sublicense to copy, distribute, display, modify, and make derivative works of Customer Materials for the purpose of providing the Value-Added Services and as may be stated in the relevant Documentation.

18.9.5 Restriction on the Use of Intellectual Property

Each Party shall not use any of the other Party's Intellectual Property except as expressly authorized in these Value-Added Services Rules and the Documentation. Other than the explicit rights granted herein, nothing in these Value-Added Services Rules shall be construed or interpreted as granting to a Party any rights or licenses, including any rights of ownership or any

other proprietary rights, in or to the other Party's Intellectual Property or any portion thereof, or any other software or technology of the other Party or its licensors, or any Intellectual Property Rights embodied within any of the foregoing. Each Party shall not, and shall not instruct, permit, allow, or induce its agents or representatives to (i) reverse engineer, decompile, or disassemble the other Party's Intellectual Property, or otherwise attempt to obtain, directly or indirectly, source code for the other Party's Intellectual Property, or attempt to discover any underlying proprietary methods or algorithms of the other Party's Intellectual Property; (ii) sell, lease, sublicense, copy, market, or distribute the other Party's Intellectual Property, except as explicitly permitted hereunder; or (iii) modify, port, translate, or create derivative works of the other Party's Intellectual Property, except as may be explicitly permitted hereunder. Each Party shall not remove or destroy any proprietary, trademark, or copyright markings contained within the other Party's Intellectual Property.

18.10 Representations and Warranties

18.10.1 General

Each Party represents and warrants that (i) it is duly organized, validly existing, and in good standing under the laws of the jurisdiction of its incorporation; (ii) it has the full right and power to enter into these Value-Added Services Rules and fully perform its obligations hereunder; and (iii) the execution and delivery of these Value-Added Services Rules and the performance of its obligations hereunder will not violate or conflict with any other agreement to which it is a party.

18.10.2 Provision and Use of Customer Items

The Customer represents and warrants that both (i) its provision of any Customer Materials, Customer Intellectual Property, or Personal Data to Mastercard or a Mastercard Supplier, or such party's receipt, in connection with the Value-Added Services, of such items from the Customer or another party; and (ii) the use, analysis, and/or processing of such items by Mastercard and/or the Mastercard Suppliers to perform and/or provide the Value-Added Services are, collectively, permitted under (x) all applicable laws, regulations, and regulatory guidance; and (y) the terms of the Customer's contracts with, notices to, or other consents from, its customers, contractors, suppliers, or other third parties.

18.10.3 Disclaimer of Warranties

All Deliverables may be developed using data, databases, systems, tools, and information (including Transactional information) provided by the Customer or third parties that may contain certain errors, omissions, or inaccuracies. Mastercard shall have no responsibility for any errors, omissions, or inaccuracies in such underlying data or in the Deliverable to the extent caused by such data.

EXCEPT AS EXPRESSLY STATED IN THESE VALUE-ADDED SERVICES RULES, ALL MASTERCARD INTELLECTUAL PROPERTY PROVIDED OR MADE AVAILABLE IS "AS IS" AND "AS AVAILABLE". TO THE FULLEST EXTENT PERMITTED BY LAW, MASTERCARD AND ITS

AFFILIATES MAKE NO WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO ANY OF THE MASTERCARD INTELLECTUAL PROPERTY OR ANY RELATED VALUE-ADDED SERVICE, OR THE USE OF OR ABILITY TO USE ANY OF THE FOREGOING, INCLUDING, WITHOUT LIMITATION: (I) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR TITLE, OR IMPLIED WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE; OR (II) THAT ANY OF THE MASTERCARD INTELLECTUAL PROPERTY WILL MEET THE CUSTOMER'S REQUIREMENTS, WILL ALWAYS BE AVAILABLE, ACCESSIBLE, UNINTERRUPTED, TIMELY, SECURE, FREE OF BUGS OR VIRUSES OR OTHER DEFECTS, OPERATE WITHOUT ERROR, OR WILL CONTAIN ANY PARTICULAR FEATURES OR FUNCTIONALITY.

18.11 Indemnification

18.11.1 Mastercard Indemnification Obligation

With respect to the Value-Added Services, Mastercard shall indemnify, defend (at its option, in accordance with Rule 18.11.3), and hold the Customer, its Affiliates, and its and their respective directors, officers, employees, agents, and representatives, harmless from and against any third party claim, and shall pay any losses, costs, liabilities, demands, damages, and expenses including reasonable attorneys' fees (collectively, **"Losses"**) incurred as a result of any such third party claim, arising out of or relating to (except to the extent caused by a Customer's breach of any of its obligations, representations, or warranties hereunder) (i) any actual or alleged infringement, violation, or misappropriation of any patent, trademark, or copyright to the extent based on any Mastercard Intellectual Property, and/or any equipment, processes, and other resources used by Mastercard in connection with the Customer Intellectual Property (other than any technology, equipment, processes, and other resources provided by the Customer); or (ii) Mastercard's (x) material breach of any of its obligations, representations, and warranties hereunder and in the applicable Documentation; or (y) gross negligence or willful misconduct in the performance of its obligations under these Value-Added Services Rules and the applicable Documentation.

18.11.2 Customer Indemnification Obligation

The Customer shall indemnify, defend (at its option, in accordance with Rule 18.11.3), and hold Mastercard, its Affiliates, and its and their respective officers, directors, employees, agents, and representatives, harmless from and against any third party claim, and shall pay any Losses incurred as a result of any such third party claim, arising out of or relating to (except to the extent caused by Mastercard's breach of any of its obligations, representations, or warranties hereunder) (i) any actual or alleged infringement, violation, or misappropriation of any patent, trademark, or copyright to the extent based on any Customer Materials, Customer Intellectual Property, and/or any equipment, processes, and other resources used by the Customer in connection with the Mastercard Intellectual Property (other than any technology, equipment, processes, and other resources provided by Mastercard); or (ii) the Customer's (x) material breach of any of its obligations, representations, and warranties hereunder; or (y) gross

negligence or willful misconduct in the performance of its obligations under these Value-Added Services Rules.

18.11.3 Indemnification Process

If a Party entitled to indemnification hereunder (the **"Indemnified Party"**) becomes aware of any claim that it believes is subject to indemnification hereunder, the Indemnified Party will give the other Party (the **"Indemnifying Party"**) prompt notice thereof. Such notice (the **"Claim Notice"**) shall (i) provide the basis on which indemnification is being asserted; and (ii) be accompanied by copies of all relevant pleadings and other papers related to the claim and in the possession of the Indemnified Party. The Indemnifying Party may assume, at its sole option, control of the defense of the claim by sending notice of such assumption to the Indemnified Party on or before thirty (30) days after receipt of the Claim Notice to acknowledge responsibility for the defense of such claim and undertake, conduct, and control, through reputable independent counsel of its own choosing and at the Indemnifying Party's sole cost and expense, the settlement or defense thereof. The Indemnified Party shall cooperate, at the expense of the Indemnifying Party, with the Indemnifying Party and its counsel in the defense, and the Indemnified Party shall have the right to participate, at its own expense, in the defense of such claim. The Indemnifying Party shall obtain the Indemnified Party's consent to any compromise or settlement of a claim to the extent such compromise or settlement affects the rights of such Indemnified Party, which consent shall not be unreasonably withheld or delayed. In addition, with respect to an indemnification claim pursuant to Rule 18.9.1 (i), Mastercard will use commercially reasonable efforts to, at its option and expense, (x) secure the right to continue to use such infringing item or service; (y) replace such item or service; or (z) modify such item or service so that it becomes non-infringing. If Mastercard is unable, on commercially reasonable terms, to procure the right to continued use of the allegedly infringing item or service, or replace or modify the allegedly infringing item or service, as provided in provisions (x) to (z) herein, the Customer or Mastercard may terminate the Value-Added Service affected by the infringing item or service. For purposes of clarity, such termination right of Mastercard is in addition to that stated in Rule 18.8.

18.12 Limitation of Liability

NOTWITHSTANDING ANY OTHER PROVISION TO THE CONTRARY SET FORTH IN THESE VALUE-ADDED SERVICES RULES, EACH PARTY SHALL NOT BE LIABLE UNDER ANY LEGAL THEORY, INCLUDING TORT, CONTRACT, STRICT LIABILITY OR OTHERWISE, FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES (INCLUDING, WITHOUT LIMITATION, TRANSACTION VALUE, CARD REISSUANCE, CARD CREDIT MONITORING, AND CARD ID THEFT PROTECTION), INCLUDING FOR LOSS OF PROFITS, DATA OR GOODWILL, REGARDLESS OF WHETHER SUCH PARTY KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

NOTWITHSTANDING ANY OTHER PROVISION TO THE CONTRARY SET FORTH IN THESE VALUE-ADDED SERVICES RULES, AND EXCLUDING LIABILITY FOR NON-PAYMENT BY THE CUSTOMER OF FEES DUE UNDER THE APPLICABLE DOCUMENTATION OR FUNDS

COVERING TRANSACTION SETTLEMENT, THE MAXIMUM AGGREGATE LIABILITY OF EACH PARTY AND ITS AFFILIATES OVER THE TERM FOR THE PROVISION OF VALUE-ADDED SERVICES (AS SET FORTH IN THE APPLICABLE DOCUMENTATION) ARISING OUT OF OR RELATING TO SUCH VALUE-ADDED SERVICES, EITHER INDIVIDUALLY OR IN A BUNDLE AS SET FORTH IN THE APPLICABLE DOCUMENTATION (INCLUDING, WITHOUT LIMITATION, INDEMNIFICATION OBLIGATIONS HEREUNDER) SHALL BE THE GREATER OF TWO HUNDRED FIFTY THOUSAND DOLLARS ($250,000) OR THE NET FEES PAID OR PAYABLE FOR THE VALUE-ADDED SERVICES BY THE CUSTOMER UNDER THE APPLICABLE DOCUMENTATION DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY.

18.13 Miscellaneous

18.13.1 Assignment

Neither Party may assign or transfer its rights or obligations granted under these Value-Added Services Rules and the Documentation, by operation of law, contract, or otherwise, without the other Party's prior written consent, such consent not to be unreasonably withheld; provided, however, that Mastercard may, without the consent of the Customer, delegate any obligations under these Value-Added Services Rules or assign these Value-Added Services Rules in whole or in part to an Affiliate capable of performing Mastercard's obligations hereunder. These Value-Added Services Rules shall be binding upon and inure to the benefit of the successors and permitted assigns of each Party.

18.13.2 Governing Law, Venue

These Value-Added Services Rules shall be governed by and construed in accordance with the laws of the State of New York, without regard to its conflicts of laws principles. Each Party irrevocably consents to the exclusive jurisdiction of the courts in Westchester County of the State of New York and the federal courts situated in the Southern District of New York, in connection with all proceedings related to these Value-Added Services Rules.

18.13.3 Publicity

Neither Party shall issue any news release, blog, media outreach, public announcement, advertisement, or any other form of publicity in connection with the Parties' relationship, these Value-Added Services, or any Documentation without first obtaining the prior written consent of the other Party.

18.13.4 Entire Agreement

These Value-Added Services Rules and the applicable Documentation constitute the entire agreement between the Customer and Mastercard with respect to the subject matter set forth in these Value-Added Services Rules. Notwithstanding the foregoing, it is expressly agreed that these Value-Added Services Rules do not and are not intended to terminate, alter, or amend any rights or any obligations from any other existing agreements between the Parties hereto that

are still in effect as of the initial publication date of these Value-Added Services Rules and until the earlier of (i) the termination of those existing agreements in accordance with their terms; or (ii) the Parties' mutual, written agreement.

18.13.5 Third Party Beneficiaries

Nothing in these Value-Added Services Rules is intended to confer any rights or remedies on any Persons other than the Parties and their permitted successors and assigns. Without limiting the foregoing, no third party shall be a beneficiary of these Value-Added Services Rules.

18.13.6 Severability

In the event that any provision of these Value-Added Services Rules conflicts with the law under which either the Enrollment Form or the applicable Documentation are to be construed or is held invalid by a court with jurisdiction over the Parties to the Enrollment Form or the applicable Documentation subjecting the Parties to these Value-Added Services Rules, (i) such provision will be deemed to be restated to reflect as nearly as possible the original intentions of the Parties in accordance with applicable law; and (ii) the remaining provisions of these Value-Added Services Rules will remain in full force and effect.

18.13.7 Force Majeure

Neither Party shall be liable for loss or damage, or for any delay, or failure to perform its obligations under these Value-Added Services Rules and/or the Documentation, to the extent such loss, damage, delay, or failure is caused by any act of God, natural disaster, fire, strike, embargo, war, threat of terrorism, insurrection, riot, denial of service attack, epidemic, pandemic or contagious disease outbreak or other cause or circumstance beyond the reasonable control of the Party; provided, however, that the foregoing shall not excuse any failure by such Party to take reasonable action to minimize the scope, extent, duration, and adverse effect of any such event.

18.13.8 Compliance

18.13.8.1 Compliance with Laws

Each Party shall fulfill its obligations as stated in these Rules in accordance with all applicable laws and regulations, including, without limitation, the Foreign Corrupt Practices Act, the U.K. Bribery Act, and all other applicable anti-corruption and anti-bribery laws. In connection with a Customer's use of the Value-Added Services and cross-border transfer of the Deliverables, the Customer shall comply with all applicable export, re-export, and import control laws and regulations of all applicable jurisdictions, and the Customer shall not export or re-export the Value-Added Services. The Customer shall not engage in any activities related to these Rules with a Person who is identified on the lists of specially designated nationals or blocked parties maintained by the U.S. Treasury Department's Office of Foreign Assets Control, or other relevant jurisdiction. Such list is currently accessible at: http://www.treasury.gov/ofac.

18.13.8.2 Compliance with Value-Added Services Rules and Documentation

Noncompliance by a Party with the specific terms and conditions applying to any of the Value-Added Services and/or applicable Documentation shall not relieve the other Party of its duty to comply with the terms and conditions relating to the other Value-Added Services and/or applicable Documentation or to suspend its performance thereof.

18.13.9 Waiver

The failure of either Party to insist upon or enforce strict performance by the other Party of any provision of these Value-Added Services Rules, or to exercise any right under these Value-Added Services Rules, shall not be construed as a waiver or relinquishment to any extent of such Party's right to assert or rely upon any such provision or right in that or any other instance; rather, the same will be and remain in full force and effect.

18.13.10 Amendment

Mastercard has the exclusive authority to modify the Value-Added Services Rules.

18.13.11 Cumulative Remedies

Except where otherwise specified, the rights and remedies granted to a Party subject to these Value-Added Services Rules in connection with its execution of an Enrollment Form or the date on which relevant Documentation otherwise becomes applicable are cumulative and in addition to, and not in lieu of, any other rights or remedies which a Party may possess at law or in equity.

18.13.12 Notices

All notices delivered under these Value-Added Services Rules shall be in writing and deemed to be given (i) when actually received if delivered personally; (ii) two (2) days after the date deposited with the U.S. Postal Service if sent by certified or registered mail; and (iii) one (1) day after the date delivered to a reputable next-day courier service. Notices shall be addressed to a Party at the address set forth on the Signature Page, to the signatory, with a copy to the General Counsel of such Party. Either Party may change such address by giving notice in accordance with this Rule.

18.13.13 Insurance

Each Party shall maintain adequate insurance or shall self-insure at an appropriate level with respect to the business activities carried out by such Party in the ordinary course. Each Party shall furnish certificates of insurance to the other Party upon reasonable request.

18.13.14 Area of Use

The Customer shall access, use, and accept provision of the Value-Added Services and Deliverables solely in the Territory.

18.13.15 Order of Precedence

With respect to those Value-Added Services in which a Customer elects to participate on or after the initial publication date of these Value-Added Services Rules, in the event of an express conflict between and among provisions of these Value-Added Services Rules, the Documentation and other Mastercard Rules, the following order of precedence shall apply, in descending order: (i) Documentation published in whole or in part on or after the initial publication of these Value-Added Services Rules; (ii) these Value-Added Services Rules; (iii) the Mastercard Rules; and (iv) existing Documentation published prior to the initial publication of these Value-Added Services Rules.

18.13.16 Survival

The expiration or termination, for any reason, of these Value-Added Services Rules will not affect (i) the rights of either Party against the other that have accrued on or prior to the termination; or (ii) any provision that, by its nature, survives the termination of these Value-Added Services Rules, including Rule 18.5 ("Confidentiality"), Rule 18.6 ("Privacy and Data Protection"), the ownership provisions within Rule 18.7, Rule 18.11 ("Indemnification"), Rule 18.12 ("Limitation of Liability"), and Rule 18.13 ("Miscellaneous"), which shall survive any termination or expiration of the Enrollment Form or applicable Documentation.

Appendix A Geographic Regions

This appendix provides listings of geographic regions.

Asia/Pacific Region

The Asia/Pacific Region includes the following countries or territories.

American Samoa	Myanmar
Australia	Nauru
Bangladesh	Nepal
Bhutan	New Caledonia
Brunei Darussalam	New Zealand
Cambodia	Niue
Christmas Island	Norfolk Island
Cocos (Keeling) Islands	Northern Mariana Islands
Cook Islands	Palau
Fiji	Papua New Guinea
French Polynesia	Philippines
Guam	Pitcairn
Heard and McDonald Islands	Samoa
Hong Kong SAR	Singapore
India	Solomon Islands
Indonesia	Sri Lanka
Japan	Taiwan
Kiribati	Thailand
Korea, Republic of	Timor-Leste
Lao People's Democratic Republic	Tokelau
Macao SAR	Tonga
Mainland China	Tuvalu
Malaysia	U.S. Minor Outlying Islands
Maldives	Vanuatu
Marshall Islands	Viet Nam
Micronesia, Federated States of	Wallis and Futuna
Mongolia	

Canada Region

The Canada Region is composed of Canada.

Europe Region

The Europe Region includes the following countries or territories.

Albania	Guernsey	Norway[3]
Andorra	Hungary	Poland
Antarctica	Iceland	Portugal[4]
Armenia	Ireland	Romania
Austria	Isle of Man	Russian Federation
Azerbaijan	Israel	San Marino
Belarus	Italy	Serbia
Belgium	Jersey	Slovakia
Bosnia and Herzegovina	Kazakhstan	Slovenia
Bulgaria	Kosovo	Spain[5]
Croatia	Kyrgyzstan	St. Helena, Ascension and Tristan Da Cunha
Cyprus	Latvia	Sweden
Czech Republic	Liechtenstein	Switzerland
Denmark[6]	Lithuania	Tajikistan
Estonia	Luxembourg	Turkey
Finland[7]	Malta	Turkmenistan
France[8]	Moldova	Ukraine
Georgia	Monaco	United Kingdom[9]
Germany	Montenegro	Uzbekistan

[3] Includes Svalbard and Jan Mayen.
[4] Includes Azores and Madeira.
[5] Includes Canary Islands, Ceuta and Melilla.
[6] Includes Faroe Islands and Greenland.
[7] Includes Aland Islands.
[8] Includes Mayotte, Guadeloupe, Martinique, French Guiana, St. Martin (French Part), Réunion, and St. Barthélemy.
[9] Includes Falkland Islands, South Georgia and South Sandwich Islands.

Gibraltar	Netherlands	Vatican City
Greece	North Macedonia	

Changes in allegiance or national affiliation of a part of any of the countries listed in this appendix shall not affect the geographic coverage of the definition.

Single European Payments Area (SEPA)

The Single European Payments Area includes the following countries or territories.

Andorra	Greece	Netherlands
Antarctica	Guernsey	Norway[10]
Austria	Hungary	Poland
Belgium	Iceland	Portugal
Bulgaria	Ireland	Romania
Croatia	Isle of Man	Saint Helena, Ascension and Tristan da Cunha
Cyprus	Italy	San Marino
Czech Republic	Jersey	Slovakia
Denmark[11]	Latvia	Slovenia
Estonia	Liechtenstein	Spain
Finland[12]	Lithuania	Sweden
France[13]	Luxembourg	Switzerland
Germany	Malta	United Kingdom[14]
Gibraltar	Monaco	Vatican City

Non-Single European Payments Area (Non-SEPA)

The Non-Single European Payments Area includes the following countries or territories.

Albania	Moldova
Armenia	Montenegro

10 Includes Svalbard and Jan Mayen.
11 Includes Faroe Islands and Greenland.
12 Includes Aland Islands.
13 Includes Mayotte, Guadeloupe, Martinique, French Guiana, St. Martin (French Part), Réunion, and St. Barthélemy.
14 Includes Falkland Islands, South Georgia and South Sandwich Islands.

Azerbaijan	North Macedonia
Belarus	Russian Federation
Bosnia and Herzegovina	Serbia
Georgia	Tajikistan
Israel	Turkey
Kazakhstan	Turkmenistan
Kosovo	Ukraine
Kyrgyzstan	Uzbekistan

Latin America and the Caribbean Region

The Latin America and the Caribbean Region includes the following countries or territories.

Anguilla	Cuba	Panama
Antigua and Barbuda	Curacao	Paraguay
Argentina	Dominica	Peru
Aruba	Dominican Republic	Puerto Rico
Bahamas	Ecuador	St. Kitts-Nevis
Barbados	El Salvador	St. Lucia
Belize	Grenada	St. Maarten
Bermuda	Guatemala	St. Vincent and the Grenadines
BES Islands[15]	Guyana	Suriname
Bolivia	Haiti	Trinidad and Tobago
Brazil	Honduras	Turks and Caicos Islands
Cayman Islands	Jamaica	Uruguay
Chile	Mexico	Venezuela
Colombia	Montserrat	Virgin Islands, British
Costa Rica	Nicaragua	Virgin Islands, U.S.

[15] Bonaire, St. Eustatius and Saba.

Middle East/Africa Region

The Middle East/Africa Region includes the following countries or territories.

Afghanistan	Gambia	Qatar
Algeria	Ghana	Rwanda
Angola	Guinea	Sao Tome and Principe
Bahrain	Guinea-Bissau	Saudi Arabia
Benin	Iraq	Senegal
Botswana	Jordan	Seychelles
Bouvet Island	Kenya	Sierra Leone
British Indian Ocean Territory	Kuwait	Somalia
Burkina Faso	Lebanon	South Africa
Burundi	Lesotho	South Sudan
Cameroon	Liberia	Sudan (excluding Darfur)
Cape Verde	Libyan Arab Jamahiriya	Swaziland
Central African Republic	Madagascar	Tanzania
Chad	Malawi	Togo
Comoros	Mali	Tunisia
Congo	Mauritania	Uganda
Côte D'Ivoire	Mauritius	United Arab Emirates
Democratic Republic of the Congo	Morocco	Western Sahara
Djibouti	Mozambique	Yemen
Egypt	Namibia	Zambia
Equatorial Guinea	Niger	Zimbabwe
Eritrea	Nigeria	
Ethiopia	Oman	
French Southern Territories	Pakistan	
Gabon	Palestine	

West African Economic and Monetary Union (UEMOA)

The West African Economic and Monetary Union includes the following countries or territories.

Benin	Mali	Togo
Burkina Faso	Niger	Guinea-Bissau
Cote d'Ivoire	Senegal	

United States Region

The United States Region is composed of the United States.

Appendix B Compliance Zones

The following table identifies the noncompliance category that the Corporation has assigned to the Standards described within this manual.

Compliance Zones

These noncompliance categories are assigned for the purposes of noncompliance assessments under the compliance framework in Rule 2.1.4.

Rule Number	Rule Title	Category
1.1	Eligibility to be a Customer	A
1.1.4	Payment Transfer Activity Customer	A
1.2	Mastercard Anti-Money Laundering and Sanctions Requirements	A
1.3	Satisfaction of Minimum Financial Requirements	A
1.4	Special Conditions of Participation, License or Activity	A
1.5	Interim Participation	A
1.6	The License	A
1.6.1	SEPA Licensing Program—Europe Region Only	A
1.7	Area of Use of the License	A
1.8	The Digital Activity Agreement	A
1.9	Participation in Activity(ies) and Digital Activity	A
1.10	Participation in Competing Networks	A
1.11	Portfolio Sale, Transfer, or Withdrawal	A
1.12	Change of Control of Customer or Portfolio	A
1.13	Termination	A
2.1.5	Certification	C
2.1.8	Rules Applicable to Intracountry Transactions	C
2.2	Conduct of Activity and Digital Activity	A
2.5	Examination and Audit	A

Compliance Zones

Rule Number	Rule Title	Category
3.1	Obligation to Issue Mastercard Cards	A
3.2	Responsibility for Transactions	A
3.3	Transaction Requirements	A
3.4	Authorization Service	A
3.5	Non-discrimination—POS Transactions	A
3.6	Non-discrimination—ATM and Bank Branch Terminal Transactions	A
3.7	Integrity of Brand and Network	A
3.8	Fees, Assessments, and Other Payment Obligations	A
3.9	Obligation of Customer to Provide Information	C
3.10	Confidential Information of Customers	A
3.12	Confidential Information of Mastercard	A
3.13	Data Protection	A
3.14	Quarterly Mastercard Report (QMR)	C
3.15	Cooperation	B
3.16	Issuer Reporting Requirement—EU, Iceland, Norway, and Serbia	C
3.17	BINs	A
3.18	Recognized Currencies	A
3.18.1	Prior Consent of the Corporation	C
3.18.2	Communications and Marketing Materials	B
4.1	Right to Use the Marks	A
4.1.1	Protection and Registration of the Marks	B
4.1.1.1	Registration of a Card Design	B
4.1.2	Misuse of a Mark	B

Compliance Zones

Rule Number	Rule Title	Category
4.2	Requirements for Use of a Mark	B
4.4	Signage System	B
4.5	Use of the Interlocking Circles Device	B
4.6	Use of Multiple Marks	B
4.7	Particular Uses of a Mark	B
4.8	Use of Marks on Maestro and Cirrus Cards	A
4.9	Use of Marks on Mastercard Cards	B
4.10	Use of a Card Design in Merchant Advertising and Signage	B
4.11	Use of a Card Design in Issuer Advertising and Marketing Material	B
4.12	Use of the Mastercard Card Design in Cardholder Statement Enclosures	B
4.13	Use of the Brand Marks on Other Cards	B
4.14	Use of EMVCo® Trademarks	B
5.1	The Merchant and ATM Owner Agreements	A
5.1.1	Verify Bona Fide Business Operation; Government Controlled Merchants	A
5.1.2	Required Merchant Agreement Terms	A
5.1.2.1	Gambling Merchants	A
5.1.3	Required ATM Owner Agreement Terms	A
5.1.4	Maintaining Information	C
5.2	Merchant and Submerchant Compliance with the Standards	A
5.3	Deferred Delivery Merchant	A
5.4	Acquirer Obligations to Merchants	B

Compliance Zones

Rule Number	Rule Title	Category
5.5	Merchant Location	A
5.6	Submerchant Location	A
5.7	Responsibility for Transactions	B
5.8	Transaction Message Data	A
5.9	Transaction Currency Information	A
5.10	Use of the Marks	B
5.11	Merchant Obligations for Acceptance	A
5.11.1	Honor All Cards	A
5.11.2	Merchant Acceptance of Mastercard Cards	A
5.11.3	Obtain an Authorization	A
5.11.4	Additional Cardholder Identification	B
5.11.5	Discounts or Other Benefits at the Point of Interaction	B
5.12	Prohibited Practices	A
5.12.1	Discrimination	A
5.12.2	Charges to Cardholders	B
5.12.3	Minimum/Maximum Transaction Amount Prohibited	B
5.12.4	Scrip-dispensing Terminals	A
5.12.5	Existing Mastercard Cardholder Obligations	A
5.12.6	Cardholder Right of Dispute	B
5.12.7	Illegal or Brand-damaging Transactions	A
5.12.8	Disparagement	A
5.12.9	Mastercard Tokens	A
5.13	Valid Transactions	A
5.14	Sale or Exchange of Information	A
5.15	Payment Account Reference (PAR) Data	A

Compliance Zones

Rule Number	Rule Title	Category
6.1	Card Issuance—General Requirements	A
6.1.1	Mastercard Card Issuance	A
6.1.2	Maestro Card Issuance	A
6.1.3	Cirrus Card Issuance	A
6.1.4	Tokenization of Accounts	A
6.1.5	Cardholder Communications	B
6.1.6	Enablement of QR-based Payments	B
6.2	Issuer Responsibilities to Cardholders	B
6.3	Limitation of Liability of Cardholders for Unauthorized Use	B
6.4	Selective Authorization	B
6.5	Affinity and Co-Brand Card Programs	A
6.5.1	Ownership and Control of the Program	A
6.5.2	Use of the Acceptance Marks	B
6.6	Brand Value Transactions and Proprietary Accounts	A
6.6.1	Proprietary Account Access	A
6.6.2	Use of BVT and Proprietary Accounts on a Mastercard Card	A
6.6.3	Fees and Reporting Requirements	C
6.7	Virtual Accounts	A
6.8	Secured Card Programs	B
6.9	Youth Card Programs	A
6.10	Prepaid Card Programs	A
6.11	Maestro Chip-only Card Programs—Europe Region Only	A
6.12	Debit Card Programs Issued by Electronic Money Institutions and Payment Institutions	A

Compliance Zones

Rule Number	Rule Title	Category
6.13	Decoupled Payment Card Programs	A
7.1	Service Provider Categories and Descriptions	A
7.2	The Program Service and Performance of Program Service	A
7.2.1	Customer Responsibility and Control	A
7.2.2	Notification to the Corporation of Change of Name or Transfer of Ownership or Control	A
7.2.3	Program Service Agreement	A
7.2.4	Disclosure of Standards	C
7.2.5	Customer Point of Contact	B
7.2.6	Use of the Marks	B
7.2.7	Service Provider Identification on a Card	B
7.2.8	Program Materials	B
7.2.9	Notification of Settlement Failure Obligation	A
7.2.10	Data Security	A
7.3	Access to Merchant Account	A
7.4	Transfer of Rights Prohibited	A
7.5	Use of Corporation's Systems and Confidential Information	A
7.6.1	Merchant Agreement	A
7.6.2	Collection of Funds from a Merchant or ATM Owner	A
7.6.3	Access to Documentation	C
7.6.4	Authority to Terminate Merchant Agreement or ATM Owner Agreement	A
7.6.5	Payment Facilitators and Submerchants	A
7.6.6	Transaction Identification for ISO and PF Transactions	A

Compliance Zones

Rule Number	Rule Title	Category
7.6.7	Staged Digital Wallet Operator Requirements	A
7.7.1	Card Application Approval	A
7.7.2	Cardholder Agreement	B
7.7.3	Program Payments	A
7.7.4	Program Receivables	A
7.7.5	Installment Service Provider Program Requirements	A
7.8	Payment Facilitator Obligations	A
7.9	Type I TPP Obligations	A
7.10	Registration and Validation Requirements for Service Providers	A
7.11.1	Network Enablement Partners Eligibility	A
7.11.2	Network Enablement Partner Agreement Requirements	A
7.11.3	Network Enablement Partner Services and Performance of Program Service	A
7.11.4	Applicability of Standards	See category assigned to underlying Rule
7.11.4.4	Testing of Assets	A
7.11.5	Network Enablement Partner Requirements	A
7.13	Termination of a Service Provider, Program Service Agreement, Network Enablement Partner Agreement or De-registration	A
7.15	Audits	C
8.2	Net Settlement	A
8.3	Interchange and Service Fees	A
8.4	Establishment of Intracountry Interchange and Service Fees	A
8.5	Failure of a Principal or Association to Discharge a Settlement Obligation	A

Compliance Zones

Rule Number	Rule Title	Category
8.6	Settlement Liability for Debit Licensees	A
8.7	Settlement Liability for Type I TPPs that Sponsor Affiliates	A
8.8	System Liquidity	A
8.9	Liability for Owned or Controlled Entities	A
8.10	Risk of Loss	A
8.11	Loss Allocation Among Customers	A
8.12	PTA Transaction Settlement	A
9.1	Digital Activity and Conduct of a Staged Digital Wallet Operator	A
9.1.2	Branding Requirements	B
9.1.3	Data Protection, Privacy and Data Usage	A
9.1.4	Security	A
9.2	DWO Requirements—Pass-through Digital Wallet	A
9.3	Digital Activity—Merchant Token Requestor	A
9.4	Digital Activity—On-behalf Token Requestor	A
10.1.1	General Requirements	A
10.1.2	Branding Requirements	B
10.1.3	Transaction Limits	A
10.1.4	Use of PTA Service	A
10.1.5	Non-Discrimination	A
10.1.6	Security Incidents	A
10.1.7	Disputes and Chargebacks	A
10.1.8	Standards of Non-Mastercard Systems and Networks	A
10.2.1	Valid Transactions	A

Compliance Zones

Rule Number	Rule Title	Category
10.2.2	Originating Institution Responsibilities to Originating Account Holders	B
10.2.3	Limitation of Liability of Originating Account Holders for Unauthorized Use	B
10.2.4	Sufficient Funds	A
10.2.5	Authentication	A
10.2.6	Irrevocability and Discharge of Settlements	A
10.3.1	Valid Transactions	A
10.3.2	Receiving Institution Responsibilities to Receiving Account Holders	A
10.3.3	Transaction Funds Availability	A

Appendix C Definitions

The following terms as used in this manual have the meanings set forth below.

Additional and/or revised terms may also be used for purposes of the Rules in a particular chapter or section of this manual.

Acceptance Mark

Any one of the Corporation's Marks displayed at a Point of Interaction (POI) to indicate brand acceptance. See Cirrus Acceptance Mark, Maestro Acceptance Mark, Mastercard Acceptance Mark.

Acceptor

The Merchant, Sponsored Merchant, ATM owner, or other entity that accepts a Card pursuant to a Merchant Agreement, Sponsored Merchant Agreement, or ATM Owner Agreement for purposes of conducting a Transaction.

Access Device

A device other than a Card that has successfully completed all applicable Mastercard certification and testing requirements, if any, and:

- Uses at least one Payment Application provisioned to the device by or with the approval of a Customer to provide access to an Account;
- Supports the transmission or exchange of data using one or both of the following:
  - Magnetic stripe or chip data containing a dynamic cryptogram to or with a Terminal, as applicable, by implementing the EMV Contactless Specifications (Book D) to effect Transactions at the Terminal without requiring direct contact of the device to the Terminal
  - Chip data containing a dynamic cryptogram to or with a Terminal, as applicable, by implementing the Mastercard Cloud-Based Payments (MCBP) documentation to effect Transactions at the Terminal by capture of a QR Code containing the Transaction Data
- May also support the transmission of magnetic stripe data containing a dynamic cryptogram to a Terminal to effect Transactions identified by the Acquirer in Transaction messages as magnetic stripe Transactions.

A Cirrus Access Device, Maestro Access Device, and Mastercard Access Device is each an Access Device. Also see Mobile Payment Device.

Access Mark

Any third party name, logo, sound, haptic, visual depiction, trade name, logotype, trademark, service mark, trade designation, and/or other designation, symbol or mark, in each case not Licensed by the Corporation, that identifies a service through which a Mastercard, Maestro, or Cirrus Account can be accessed and/or accepted for a Transaction.

Account

An account maintained by or on behalf of a Cardholder by an Issuer for the processing of Transactions, and which is identified with a bank identification number (BIN) or Issuer identification number (IIN) designated by the Corporation in its routing tables for routing to the Interchange System. Also see Cirrus Account, Maestro Account, Mastercard Account.

Account Holder

A user who holds a PTA Account and has agreed to participate in a PTA Transaction.

Account PAN

The primary account number (PAN) allocated to an Account by an Issuer.

Account PAN Range

The range of Account PANs designated by an Issuer for Digitization.

Acquirer

A Customer in its capacity as an acquirer of a Transaction.

Activity(ies)

The undertaking of any lawful act that can be undertaken only pursuant to a License granted by the Corporation. Payment Transfer Activity is a type of Activity. Also see Digital Activity(ies).

Affiliate Customer, Affiliate

A Customer that participates indirectly in Activity through the Sponsorship of a Principal or, solely with respect to Mastercard Activity, through the Sponsorship of an Association. An Affiliate may not Sponsor any other Customer.

Applicable Data Protection Law

All applicable law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation or rule (each as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which the Parties are subject, including but not limited to the EU General Data Protection Regulation 2016/679; the e-Privacy Directive 2002/58/EC and their national implementing legislations the California Consumer Privacy Act; the U.S. Gramm-Leach-Bliley Act; the Brazil General Data Protection Act; the South Africa Protection of Personal Information Act; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws governing the portability and/or cross-border transfer of Personal Data; and all other similar international, federal, state, provincial, and local requirements; each as applicable.

Area of Use

The country or countries in which a Customer is Licensed to use the Marks and conduct Activity or in which a PTA Customer is permitted to Participate in a PTA Program, and, as a rule, set forth in the License or PTA Agreement or in an exhibit to the License or PTA Agreement.

Association Customer, Association

A Mastercard Customer that participates directly in Mastercard Activity using its assigned BINs and which may Sponsor one or more Mastercard Affiliates but may not directly issue Mastercard Cards or acquire Mastercard Transactions, or in the case of a PTA Association, may not directly hold PTA Accounts, without the express prior written consent of the Corporation.

ATM Access Fee

A fee charged by an Acquirer in connection with a cash withdrawal or Shared Deposit Transaction initiated at the Acquirer's ATM Terminal with a Card, and added to the total Transaction amount transmitted to the Issuer.

ATM Owner Agreement

An agreement between an ATM owner and a Customer that sets forth the terms pursuant to which the ATM accepts Cards.

Automated Teller Machine (ATM)

An unattended self-service device that performs basic banking functions such as accepting deposits, cash withdrawals, ordering transfers among accounts, loan payments and account balance inquiries.

ATM Terminal

An ATM that enables a Cardholder to effect an ATM Transaction with a Card (and if contactless-enabled, an Access Device) in accordance with the Standards.

ATM Transaction

A cash withdrawal effected at an ATM Terminal with a Card and processed through the Mastercard® ATM Network. An ATM Transaction is identified with MCC 6011 (Automated Cash Disbursements—Customer Financial Institution).

Bank Branch Terminal

An attended device, located on the premises of a Customer or other financial institution designated as its authorized agent by the Corporation, that facilitates a Manual Cash Disbursement Transaction by a Cardholder.

BIN

A bank identification number (BIN, sometimes referred to as an Issuer identification number, or IIN) is a unique number assigned by Mastercard for use by a Customer in accordance with the Standards.

Brand Fee

A fee charged for certain Transactions not routed to the Interchange System.

Brand Mark

A Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Mastercard Brand Mark, Maestro Brand Mark, and Cirrus Brand Mark is each a Brand Mark. The Mastercard Symbol is also a Brand Mark.

Card

A card issued by a Customer pursuant to License and in accordance with the Standards and that provides access to an Account. Unless otherwise stated herein, Standards applicable to the use and acceptance of a Card are also applicable to an Access Device and, in a Card-not-present environment, an Account. A Cirrus Card, Maestro Card, and Mastercard Card is each a Card.

Cardholder

The authorized user of a Card or Access Device issued by a Customer.

Cardholder Communication

Any communication by or on behalf of an Issuer to a Cardholder or prospective Cardholder. A Solicitation is one kind of Cardholder Communication.

Cardholder Verification Method (CVM)

A process used to confirm that the person presenting the Card is an authorized Cardholder. The Corporation deems the following to be valid CVMs when used in accordance with the Standards:

- Signature CVM – The Merchant or Acquirer accepting the Card has the option to collect the Cardholder's signature;
- PIN CVM – The comparison, by the Card Issuer or the EMV chip on the Card, of the value entered on a Terminal's PIN pad with the personal identification number (PIN) given to or selected by the Cardholder upon Card issuance; and
- Consumer Device CVM (CDCVM) – The use of a CDCVM that Mastercard approved as a valid CVM for Transactions upon the successful completion of the certification and testing procedures set forth in section 3.11 of the *Security Rules and Procedures*.

In certain Card-present environments, a Merchant may complete the Transaction without a CVM ("no CVM" as the CVM), such as in Contactless Transactions less than or equal to the CVM limit, and Transactions at an unattended Point-of-Sale (POS) Terminal identified as Cardholder-activated Terminal (CAT) Level 2 or Level 3.

China Switch Manual Transaction

A China domestic Transaction manually initiated by the Acquirer using the China Dispute Resolution Platform, that includes manual preauthorization reversal, manual preauthorization complete and manual refund.

Chip Card (Smart Card, Integrated Circuit Card, IC Card, or ICC)

A Card with an embedded EMV-compliant chip containing memory and interactive capabilities used to identify and store additional data about a Cardholder, an Account, or both.

Chip-only MPOS Terminal

An MPOS Terminal that has a contact chip reader and no magnetic stripe-reading capability and that must:

1. Operate as an online-only POS Terminal for authorization purposes;
2. Support either signature CVM or No CVM as a Cardholder Verification Method, and may also support PIN verification if conducted by means of a PIN entry device (PED) that is in compliance with the Payment Card Industry (PCI) POS PED Security Requirements and Evaluation Program; and
3. Otherwise comply with the Corporation's requirements for Hybrid POS Terminals.

Chip Transaction

A Contact Chip Transaction or a Contactless Transaction.

Cirrus Acceptance Mark

A Mark consisting of the Cirrus Brand Mark placed on the dark blue acceptance rectangle, available at www.mastercardbrandcenter.com.

Cirrus Access Device

An Access Device that uses at least one Cirrus Payment Application to provide access to a Cirrus Account when used at an ATM Terminal or Bank Branch Terminal.

Cirrus Account

An account eligible to be a Cirrus Account and identified with a BIN/IIN associated with a Portfolio designated by the Corporation as a Cirrus Portfolio in its routing tables.

Cirrus Brand Mark

A Mark consisting of the Cirrus Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Corporation is the exclusive owner of the Cirrus Brand Mark.

Cirrus Card

A Card that provides access to a Cirrus Account.

Cirrus Customer

A Customer that has been granted a Cirrus License in accordance with the Standards.

Cirrus Payment Application

A Payment Application that stores Cirrus Account data.

Cirrus Word Mark

A Mark consisting of the word "Cirrus" followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent. "Cirrus" must appear in English and be spelled correctly, with the letter "C" capitalized. "Cirrus" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. The Corporation is the exclusive owner of the Cirrus Word Mark.

Competing ATM Network

A Competing International ATM Network or a Competing North American ATM Network, as the case may be.

Competing International ATM Network

A network of ATMs and payment cards, other than the Corporation, identified by a common brand mark that is used exclusively or primarily for ATM interchange that:

1. Operates in at least three countries;
2. Uses a common service mark or marks to identify the ATMs and payment cards which provide account access through it; and

3. Provides account access to at least 40,000,000 debit cards and by means of at least 25,000 ATMs.

Competing EFT POS Network

A network, other than any network owned and operated by the Corporation, which provides access to Maestro Accounts at POS Terminals by use of payment cards and has the following characteristics:

1. It provides a common service mark or marks to identify the POS Terminal and payment cards, which provide Maestro Account access;
2. It is not an affiliate of the Corporation; and
3. It operates in at least one country in which the Corporation has granted a License or Licenses.

The following networks are designated without limitation to be Competing EFT POS Networks: Interlink; Electron; and V-Pay.

Competing North American ATM Network

A network of ATMs and access cards, other than the Corporation, identified by a common brand mark that is used exclusively or primarily for ATM interchange and that possesses each of the following characteristics:

1. It operates in at least 40 of the states or provinces of the states and provinces of the United States and Canada;
2. It uses a common service mark or common service marks to identify the terminals and cards which provide account access through it;
3. There are at least 40,000,000 debit cards that provide account access through it; and
4. There are at least 12,000 ATMs that provide account access through it.

Consumer Device Cardholder Verification Method, Consumer Device CVM, CDCVM

A CVM that occurs when personal credentials established by the Cardholder to access an Account by means of a particular Access Device are entered on the Access Device and verified, either within the Access Device or by the Issuer during online authorization. A CDCVM is valid if the Issuer has approved the use of the CVM for the authentication of the Cardholder.

Contact Chip Transaction

A Transaction in which data is exchanged between the Chip Card and the Terminal through the reading of the chip using the contact interface, in conformance with EMV specifications.

Contactless Payment Device

A means other than a Card by which a Cardholder may access an Account at a Terminal in accordance with the Standards. A Contactless Payment Device is a type of Access Device that exchanges data with the Terminal by means of radio frequency communications. Also see Mobile Payment Device.

Contactless Transaction

A Transaction in which data is exchanged between the Chip Card or Access Device and the Terminal through the reading of the chip using the contactless interface, by means of radio frequency communications. Also see EMV Mode Contactless Transaction, Magnetic Stripe Mode Contactless Transaction.

Control, Controlled

As used herein, Control has such meaning as the Corporation deems appropriate in its sole discretion given the context of the usage of the term and all facts and circumstances the Corporation deems appropriate to consider. As a general guideline, Control often means to have, alone or together with another entity or entities, direct, indirect, legal, or beneficial possession (by contract or otherwise) of the power to direct the management and policies of another entity.

Corporation

Mastercard International Incorporated, Maestro International Inc., and their subsidiaries and affiliates. As used herein, Corporation also means the President and Chief Executive Officer of Mastercard International Incorporated, or his or her designee, or such officers or other employees responsible for the administration and/or management of a program, service, product, system or other function. Unless otherwise set forth in the Standards, and subject to any restriction imposed by law or regulation, or by the Board of Directors of Mastercard International Incorporated, or by the Mastercard International Incorporated Certificate of Incorporation or the Mastercard Incorporated Certificate of Incorporation (as each such Certificate of Incorporation may be amended from time to time), each such person is authorized to act on behalf of the Corporation and to so act in his or her sole discretion.

Corporation Asset

A Corporation ICA and/or BIN or BIN range.

Corporation System

The Interchange System as defined in this manual.

Cross-border Transaction

A Transaction that occurs at a Card acceptance location in a different country from the country in which the Card was issued.

Customer

A financial institution or other entity that has been approved for Participation. A Customer may be a Principal, Association, Affiliate, Digital Activity Customer, Sponsored Digital Activity Entity, or PTA Customer. Also see Cirrus Customer, Maestro Customer, Mastercard Customer, Member.

Customer Report

Any report that a Customer is required to provide to the Corporation, whether on a one-time or repeated basis, pertaining to its License, Activities, Digital Activity Agreement, Digital Activities, PTA Agreement, Payment Transfer Activities, use of any Mark, or any such matters. By way of example and not limitation, the Quarterly Mastercard Report (QMR) is a Customer Report.

Data Storage Entity (DSE)

A Service Provider that performs any one or more of the services as DSE Program Service.

Data Subject

A Cardholder or other natural person or entity whose Personal Data is Processed in the context of Activity or Digital Activity.

Device Binding

The process by which a Wallet Token Requestor binds a Mastercard Token corresponding to a Cardholder's Account to that Cardholder's Mobile Payment Device, which may consist of:

- The provisioning of the Token and its associated encryption keys into the secure element within the Mobile Payment Device;
- The loading of an application for a remotely-managed secure server into the Mobile Payment Device and the successful communication of the device with the application; or
- Other methodology acceptable to the Corporation.

Digital Activity(ies)

The undertaking of any lawful act pursuant to approval by the Corporation as set forth in a Digital Activity Agreement or other written documentation. Participation in the Mastercard Digital Enablement Service as a Wallet Token Requestor is a Digital Activity.

Digital Activity Agreement

The contract between the Corporation and a Digital Activity Customer granting the Digital Activity Customer the right to participate in Digital Activity and a limited License to use one or more of the Marks in connection with such Digital Activity, in accordance with the Standards.

Digital Activity Customer

A Customer that participates in Digital Activity pursuant to a Digital Activity Agreement and which may not issue Cards, acquire Transactions, or Sponsor any other Customer into the Corporation.

Digital Activity Service Provider (DASP)

A Service Provider that performs any one or more of the services as DASP Program Service.

Digital Activity Sponsoring Customer

A Principal Customer or Digital Activity Customer that sponsors a Sponsored Digital Activity Entity to participate in Digital Activity.

Digital Goods

Any goods that are stored, delivered, and used in electronic format, such as, by way of example but not limitation, books, newspapers, magazines, music, games, game pieces, and software (excluding gift cards). The delivery of a purchase of Digital Goods may occur on a one-time or subscription basis.

Digital Wallet

A Pass-through Digital Wallet or a Staged Digital Wallet.

Digital Wallet Operator (DWO)

A Service Provider that operates a Staged Digital Wallet or a Customer that operates a Pass-through Digital Wallet. A Merchant that stores Mastercard or Maestro Account data solely on its own behalf to effect Transactions initiated by the consumer is not deemed to be a DWO.

Digital Wallet Operator Mark, DWO Mark

A Mark identifying a particular Pass-through Digital Wallet and/or Staged Digital Wallet, and which may be displayed at the POI to denote that a retailer, or any other person, firm, or corporation, accepts payments effected by means of that Pass-through Digital Wallet and/or Staged Digital Wallet. A "Staged DWO Mark" and a "Pass-through DWO Mark" are both types of DWO Marks.

Digital Wallet Operator (DWO) Security Incident, DWO Security Incident

Any incident pertaining to the unintended or unlawful disclosure of Personal Data in connection with such Personal Data being processed through a DWO.

Digitization, Digitize

Data preparation performed by, or on behalf of, an Issuer prior to the provisioning of Account credentials or a PTA Customer prior to the provisioning of PTA Account credentials, in the form of a Mastercard Token, onto a Payment Device or into a server. Digitization includes Tokenization.

Domestic Transaction

See Intracountry Transaction.

Dual Interface

The description of a Terminal or Card that is capable of processing Contactless Transactions by means of its contactless interface and Contact Chip Transactions by means of its contact interface.

Electronic Money

Electronically (including magnetically) accessed monetary value as represented by a claim on the Electronic Money Issuer which:

1. Is issued on receipt of funds for the purpose of making transactions with payment cards; and
2. Is accepted by the Electronic Money Issuer or a person other than the Electronic Money Issuer.

Electronic Money Issuer

An Electronic Money Institution with respect only to its issuing activities.

Electronic Money Institution

An entity authorized by applicable regulatory authority or other government entity as an "electronic money institution", "e-money institution", "small electronic money institution", or any other applicable qualification under which an entity is authorized to issue or acquire Electronic Money transactions under applicable law or regulation.

EMV Mode Contactless Transaction

A Contactless Transaction in which the Terminal and the chip exchange data, enabling the chip to approve the Transaction offline on the Issuer's behalf or to request online authorization from the Issuer, in compliance with the Standards.

End User

Recipients of any lending services from the Installment Service Provider in accordance with an Installment Lending Agreement. An End User can be a natural person or an entity.

Funding Transaction

A Funding Transaction is a Point-of-Sale (POS) Transaction for the purchase of funds transfer services that involves the transfer of funds from an eligible Account by an Acquirer on behalf of the Cardholder (directly or indirectly) for the purpose of either: (a) funding a subsequent and linked funds transfer from the Cardholder to another person or entity or (b) transferring funds into another eligible financial account held by that same Cardholder. Eligible Accounts and eligible financial accounts are set out in the *Mastercard MoneySend and Funding Transactions Program Standards*.

Gaming Payment Transaction

A type of Payment Transaction that transfers winnings or value usable for gambling or gaming to a Mastercard or Maestro Account.

Gateway Customer

A Customer that uses the Gateway Processing service.

Gateway Processing

A service that enables a Customer to forward a Gateway Transaction to and/or receive a Gateway Transaction from the Mastercard® ATM Network.

Gateway Transaction

An ATM transaction effected with a payment card or other access device not bearing a Mark that is processed through or using the Mastercard® ATM Network.

Global Collection Only (GCO) Data Collection Program

A program of the Corporation pursuant to which a Customer must provide collection-only reporting of non-Processed Transactions effected with a Card, Access Device, or Account issued

under a Mastercard-assigned BIN using the Corporation's Global Clearing Management System (GCMS), in accordance with the requirements set forth in the *Mastercard Global Collection Only* manual.

Government Controlled Merchant

A Merchant that is a government entity or an entity that is at least fifty percent (50%) owned or controlled (either directly, indirectly, legally or beneficially) by a government or government entity.

Host Card Emulation (HCE)

The presentation on a Mobile Payment Device of a virtual and exact representation of a Chip Card using only software on the Mobile Payment Device and occurring by means of its communication with a secure remote server.

Hybrid Terminal

A Terminal, including any POS or MPOS Terminal ("Hybrid POS Terminal", "Hybrid MPOS Terminal"), ATM Terminal ("Hybrid ATM Terminal"), or Bank Branch Terminal ("Hybrid Bank Branch Terminal"), that:

1. Is capable of processing both Contact Chip Transactions and magnetic stripe Transactions;
2. Has the equivalent hardware, software, and configuration as a Terminal with full EMV Level 1 and Level 2 type approval status with regard to the chip technical specifications; and
3. Has satisfactorily completed the Corporation's Terminal Integration Process (TIP) in the appropriate environment of use.

ICA

A unique number assigned by the Corporation to identify a Customer in relation to Activity.

Identification & Verification (ID&V)

The identification and verification of a person as the Cardholder to whom the Issuer allocated the Account PAN to be Tokenized.

Independent Sales Organization (ISO)

A Service Provider that performs any one or more of the services as ISO Program Service.

Installment Lending Agreement

The agreement between the Installment Service Provider and an End User, which includes terms and conditions governing the relationship between the parties, such as lending amount and repayment terms.

Interchange System

The computer hardware and software operated by and on behalf of the Corporation for the routing, processing, and settlement of Transactions and PTA Transactions including, without limitation, the Mastercard Network, the Mastercard ATM Network, the Dual Message System, the Single Message System, the Global Clearing Management System (GCMS), the Settlement Account Management (SAM) system, and the China Switch system.

Inter-European Transaction

A Transaction completed using a Card issued in a country or territory listed in Single European Payments Area (SEPA) at a Terminal located in a country or territory listed in Non-Single European Payments Area (Non-SEPA) or Transaction completed using a Card issued in a country or territory listed in Non-Single European Payments Area (Non–SEPA) at a Terminal located in a country or territory listed in Single European Payments Area (SEPA).

Interregional Transaction

A Transaction that occurs at a Card acceptance location in a different Region from the Region in which the Card was issued. In the Europe Region, the term "Interregional Transaction" includes any "Inter-European Transaction," as such term is defined in the "Europe Region" chapter of the *Mastercard Rules*.

Intracountry Transaction

A Transaction that occurs at a Card acceptance location in the same country as the country in which the Card was issued. A Transaction conducted with a Card bearing one or more of the Brand Marks, either alone or in combination with the marks of another payment scheme, and processed as a Transaction, as shown by the Card type identification in the Transaction record, using either the Interchange System or a different network, qualifies as an Intracountry Transaction. "Domestic Transaction" is an alternative term for Intracountry Transaction.

Intra–European Transaction

An Intra-Non-SEPA Transaction or an Intra–SEPA Transaction, but not an Inter–European Transaction.

Intra–Non–SEPA Transaction

A Transaction completed using a Card issued in a country or territory listed in Non–Single European Payments Area (Non–SEPA) at a Terminal located in a country or territory listed in Non–Single European Payments Area (Non–SEPA).

Intraregional Transaction

A Transaction that occurs at a Card acceptance location in a different country from the country in which the Card was issued, within the same Region. In the Europe Region, this term is replaced by "Intra-European Transaction," as such term is defined in the "Europe Region" chapter of the *Mastercard Rules*.

Issuer

A Customer in its capacity as an issuer of a Card or Account.

License, Licensed

The contract between the Corporation and a Customer granting the Customer the right to use one or more of the Marks in accordance with the Standards and in the case of Payment Transfer Activity, includes a PTA Agreement. To be "Licensed" means to have such a right pursuant to a License.

Licensee

A Customer or other person authorized in writing by the Corporation to use one or more of the Marks.

Maestro

Maestro International Incorporated, a Delaware U.S.A. corporation or any successor thereto.

Maestro Acceptance Mark

A Mark consisting of the Maestro Brand Mark placed on the dark blue acceptance rectangle, as available at www.mastercardbrandcenter.com.

Maestro Access Device

An Access Device that uses at least one Maestro Payment Application to provide access to a Maestro Account when used at a Terminal.

Maestro Account

An account eligible to be a Maestro Account and identified with a BIN/IIN associated with a Portfolio designated by the Corporation as a Maestro Portfolio in its routing tables.

Maestro Brand Mark

A Mark consisting of the Maestro Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Corporation is the exclusive owner of the Maestro Brand Mark.

Maestro Card

A Card that provides access to a Maestro Account.

Maestro Customer

A Customer that has been granted a Maestro License in accordance with the Standards.

Maestro Payment Application

A Payment Application that stores Maestro Account data.

Maestro Word Mark

A Mark consisting of the word "Maestro" followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent.

"Maestro" must appear in English and be spelled correctly, with the letter "M" capitalized. "Maestro" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. Maestro is the exclusive owner of the Maestro Word Mark.

Magnetic Stripe Mode Contactless Transaction

A Contactless Transaction in which the Terminal receives static and dynamic data from the chip and constructs messages that can be transported in a standard magnetic stripe message format, in compliance with the Standards.

Mainland China Deposit Transaction

A domestic deposit to an Account conducted at an ATM Terminal located in Mainland China, initiated with a Card issued by a Mainland China Customer, and processed through the China Switch.

Mainland China Funds Transfer Funding Transaction

A domestic financial transaction sent by the China Switch on behalf of the Originating Institution to the Funding Institution to fund the subsequent associated Mainland China Funds Transfer Payment Transaction.

Mainland China Funds Transfer Payment Transaction

A domestic financial transaction sent by the China Switch on behalf of the Originating Institution to the Receiving Institution to transfer the funds into a receiving account.

Mainland China Funds Transfer Request

A domestic non-financial transaction sent by the Originating Institution to the China Switch to initiate the Mainland China Funds Transfer Transactions.

Mainland China Funds Transfer Transaction

Mainland China domestic Transactions that facilitates the funds transfer from an Account to another Account. Each Mainland China Funds Transfer Transaction contains two associated transactions, the Mainland China Funds Transfer Funding Transaction and the Mainland China Funds Transfer Payment Transaction.

Mastercard China Domestic Application

Mastercard China Domestic Application (MCDA) is Mastercard designed chip card application following PBoC chip standards, which is following Mainland China Financial Integrated Circuit Card Specifications. All chip cards issued by Mainland China issuers contain both PBoC and EMV applications. All Mainland China domestic chip transactions must be completed by PBoC application.

Mainland China Recurring Payment Transaction – Recurring Payment Terms

The recurring payment terms are the terms and conditions agreed by Merchant and Cardholder for Mainland China domestic recurring payment Transactions. It includes card acceptor name, merchandise or service, payment account, recurring payment frequency or condition, and ending date (if applicable). The Acquirer must populate the recurring payment terms in each Mainland China domestic recurring payment Transaction message.

Manual Cash Disbursement Transaction

A disbursement of cash performed upon the acceptance of a Card by a Customer financial institution teller. A Manual Cash Disbursement Transaction is identified with MCC 6010 (Manual Cash Disbursements—Customer Financial Institution).

Marks

The names, logos, sounds, animations, haptics, visual depictions, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks that the Corporation owns, manages, licenses, or otherwise Controls and makes available for use by Customers and other authorized entities in accordance with a License. A "Mark" means any one of the Marks.

Mastercard

Mastercard International Incorporated, a Delaware U.S.A. corporation.

Mastercard Acceptance Mark

A Mark consisting of the Mastercard Brand Mark or Mastercard Symbol placed on the dark blue acceptance rectangle, as available at www.mastercardbrandcenter.com.

Mastercard Access Device

An Access Device that uses at least one Mastercard Payment Application to provide access to a Mastercard Account when used at a Terminal.

Mastercard Account

Any type of account (credit, debit, prepaid, commercial, etc.) identified as a Mastercard Account with a primary account number (PAN) that begins with a BIN in the range of 222100 to 272099 or 510000 to 559999.

Mastercard Biometric Card

A Mastercard or Maestro Chip Card containing a fingerprint sensor and compliant with the Corporation's biometric Standards.

Mastercard-branded Application Identifier (AID)

Any of the Corporation's EMV chip application identifiers for Mastercard, Maestro, and Cirrus Payment Applications as defined in the *M/Chip Requirements for Contact and Contactless* manual.

Mastercard Brand Mark

A Mark consisting of the Mastercard Word Mark as a custom lettering legend placed within the Mastercard Interlocking Circles Device. The Corporation is the exclusive owner of the Mastercard Brand Mark. The Mastercard Symbol is also a Mastercard Brand Mark.

Mastercard Card

A Card that provides access to a Mastercard Account.

Mastercard Cloud-Based Payments

A specification that facilitates the provisioning of Digitized Account data into a Host Card Emulation (HCE) server and the use of the remotely stored Digitized Account data, along with single-use payment credentials, in Transactions effected by a Cardholder using a Mobile

Payment Device. The Mastercard Digital Enablement Service offers Mastercard Cloud-Based Payments as an on-behalf service.

Mastercard Consumer-Presented QR Transaction

A Mastercard Consumer-Presented QR Transaction is an EMV Chip Transaction effected through the presentment of a QR Code by the Cardholder, using a Mobile Payment Device, and the capture of the QR Code by the Merchant containing the Transaction Data required to initiate a Transaction.

Each Mastercard Consumer-Presented QR Transaction must comply with all requirements set forth in the Standards applicable to a Mastercard Consumer-Presented QR Transaction, including but not limited to those herein, in the technical specifications for authorization messages, in the *M/Chip Requirements for Contact and Contactless* manual, and in the Mastercard Cloud-Based Payments (MCBP) documentation.

Mastercard Customer

A Customer that has been granted a Mastercard License in accordance with the Standards. Also see Member.

Mastercard Digital Enablement Service

Any of the services offered by the Corporation exclusively to Customers for the digital enablement of Account and/or PTA Account data, including but not limited to ID&V Service, Tokenization Service, Digitization Service, Token Mapping Service, Mastercard Cloud-Based Payments, Digital Card Image Database, CVC 3 pre-validation and other on-behalf cryptographic validation services, and Service Requests.

Mastercard Europe

Mastercard Europe SA, a Belgian private limited liability (company).

Mastercard Incorporated

Mastercard Incorporated, a Delaware U.S.A. corporation.

Mastercard Payment Application

A Payment Application that stores Mastercard Account data.

Mastercard Safety Net

A service offered by the Corporation that performs fraud monitoring at the network level for all Transactions processed on the Mastercard Network. The service invokes targeted measures to provide protective controls on behalf of a participating Issuer to assist in minimizing losses in the event of a catastrophic fraud attack.

Mastercard Symbol

A Mark consisting of the Mastercard interlocking circles device. The Corporation is the exclusive owner of the Mastercard Symbol. The Mastercard Symbol is also a Mastercard Brand Mark.

Mastercard Token

A Token allocated from a Mastercard Token Account Range that the Corporation has designated to an Issuer or PTA Customer and that corresponds to an Account PAN or a PTA Account Number. The Corporation exclusively owns all right, title, and interest in any Mastercard Token.

Mastercard Token Account Range

A bank identification number (BIN) or portion of a BIN ("BIN range") designated by the Corporation to an Issuer or PTA Customer for the allocation of Mastercard Tokens in a particular Token implementation. A Mastercard Token Account Range must be designated from a BIN reserved for the Corporation by the ISO Registration Authority and for which the Corporation is therefore the "BIN Controller," as such term is defined in the EMV Payment Tokenization Specification Technical Framework (also see the term "Token BIN Range" in that document). A Mastercard Token Account Range is identified in the Corporation's routing tables as having the same attributes as the corresponding Account PAN Range or the range of PTA Account Numbers.

Mastercard Token Vault

The Token Vault owned and operated by Mastercard and enabled by means of the Mastercard Digital Enablement Service.

Mastercard Word Mark

A Mark consisting of the word "Mastercard" followed by a registered trademark ® symbol or the local law equivalent. "Mastercard" must appear in English and be spelled correctly, with the

letter "M" capitalized. "Mastercard" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. The Corporation is the exclusive owner of the Mastercard Word Mark.

Member, Membership

A financial institution or other entity that is approved to be a Mastercard Customer in accordance with the Standards and which, as a Mastercard Customer, has been granted membership ("Membership") in and has become a member ("Member") of the Corporation. "Membership" also means "Participation".

Merchandise Transaction

The purchase by a Cardholder of merchandise or a service, but not currency, in an approved category at an ATM Terminal and dispensed or otherwise provided by such ATM Terminal. A Merchandise Transaction is identified with MCC 6012 (Merchandise and Services—Customer Financial Institution), unless otherwise specified.

Merchant

A retailer, or any other person, firm or corporation that, pursuant to a Merchant Agreement, agrees to accept Cards when properly presented.

Merchant Agreement

An agreement between a Merchant and a Customer that sets forth the terms pursuant to which the Merchant is authorized to accept Cards.

Merchant Card-on-File Tokenization

The use of the Mastercard Digital Enablement Service (MDES) to replace Mastercard or Maestro Account data (meaning PAN and expiration date), that the Cardholder expressly authorized a Merchant to store for use in a future Transaction, with a Mastercard Token.

Merchant Token Requestor

A Merchant approved by the Corporation to conduct Digital Activity and authorized to connect directly or indirectly to the Mastercard Digital Enablement Service (MDES) for the purpose of Tokenizing a Mastercard or Maestro Account primary account number (PAN) provided by a

Cardholder for use in a future Transaction with the Merchant. A Merchant Token Requestor is a type of Token Requestor.

Mobile Payment Device

A Cardholder-controlled mobile device containing a Payment Application compliant with the Standards, and which uses an integrated keyboard and screen to access an Account. A Mobile Payment Device may also be a Contactless Payment Device or a Mastercard Consumer-Presented QR payment device.

Mobile POS (MPOS) Terminal

An MPOS Terminal enables a mobile device to be used as a POS Terminal. Card "reading" and software functionality that meets the Corporation's requirements may reside within the mobile device, on a server accessed by the mobile device, or in a separate accessory connected (such as using Bluetooth or a USB port) to the mobile device. The mobile device may be any multi-purpose mobile computing platform, including, by way of example and not limitation, a feature phone, smart phone, tablet, or personal digital assistant (PDA).

MoneySend Payment Transaction

A type of Payment Transaction that is effected pursuant to, and subject to, the MoneySend Standards.

Multi-Account Chip Card

A Chip Card with more than one Account encoded in the chip.

Network Enablement Partner

A Service Provider that executes a Network Enablement Partner Agreement as agreed by the Corporation.

Network Enablement Partner Agreement

The agreement between the Corporation and a Service Provider granting such Service Provider the right to be a Network Enablement Partner.

Non-Mastercard Funding Source

Any funding source used to fund a PTA Transaction other than an Account.

Non-Mastercard Receiving Account

Any receiving account used to receive a PTA Transaction other than an Account.

Non-Mastercard Systems and Networks Standards

The applicable rules, regulations, by-laws, standards, procedures, and any other obligations or requirements of an applicable payment network or system that is not owned, operated, or controlled by the Corporation.

On-behalf Token Requestor

A Digital Activity Customer or other Customer, Service Provider, or other entity approved by the Corporation to conduct Digital Activity and authorized to Tokenize a Mastercard or Maestro primary account number (PAN) using the Mastercard Digital Enablement Service (MDES) on behalf of a DWO or Merchant. Also called a Token Aggregator.

On-Device Cardholder Verification

The use of a CDCVM as the CVM for a Transaction.

Originating Account Holder

The Account Holder originating the PTA Transaction.

Originating Institution (OI)

A PTA Customer that Participates in a Payment Transfer Activity as an originator of PTA Transactions.

Ownership, Owned

As used herein, ownership has such meaning as the Corporation deems appropriate in its sole discretion given the context of the usage of the term in all facts and circumstances the Corporation deems appropriate to consider. As a general guideline, ownership often means to own indirectly, legally, or beneficially more than fifty percent (50 percent) of an entity.

Participation

The right to participate in Activity, Digital Activity, and/or Payment Transfer Activity granted to a Customer by the Corporation. For a Mastercard Customer, Participation is an alternative term for Membership.

Pass-through Digital Wallet

Functionality which can be used at more than one Merchant, and by which the Pass-through Digital Wallet Operator stores Mastercard or Maestro Account data provided by the Cardholder to the DWO for purposes of effecting a payment initiated by the Cardholder to a Merchant or Submerchant, and upon the performance of a Transaction, transfers the Account data to the Merchant or Submerchant or to its Acquirer or the Acquirer's Service Provider.

Pass-through Digital Wallet Operator (DWO)

A Digital Activity Customer or other Customer, approved by the Corporation to engage in Digital Activity, that operates a Pass-through Digital Wallet.

Payment Account Reference (PAR)

A unique non-financial alphanumeric value assigned to an Account PAN or PTA Account Number that is used to link the Account PAN or PTA Account Number to all of its corresponding Tokens.

Payment Application

A package of code and data stored in a Card, an Access Device, a server, or a combination of Access Device and server, that when exercised outputs a set of data that may be used to effect a Transaction, in accordance with the Standards. A Mastercard Payment Application, Maestro Payment Application, and Cirrus Payment Application is each a Payment Application.

Payment Facilitator

A Service Provider registered by an Acquirer to facilitate the acquiring of Transactions by the Acquirer from Submerchants, and which in doing so, performs any one or more of the services as PF Program Service.

Payment Transaction

A PTA Transaction that transfers funds to an Account. A Payment Transaction is not a credit that reverses a previous purchase. Includes MoneySend Payment Transaction and Gaming Payment Transaction.

Payment Transfer Activity(ies) (PTA)

The undertaking of any lawful act that can be undertaken only pursuant to a PTA Agreement or pursuant to a License granted by the Corporation. Participation in a PTA Program is Payment Transfer Activity.

Personal Data

Any information relating to an identified or identifiable individual, including contact information, demographic information, passport number, Social Security number or other national identification number, bank account information, account number (for example, Primary Account Number) and authentication information (e.g. identification codes, passwords).

Point of Interaction (POI)

The location at which a Transaction occurs or a PTA Transaction originates, as determined by the Corporation.

Point-of-Sale (POS) Terminal

One of the following:

- An attended or unattended device, including any commercial off-the-shelf (COTS) or other device enabled with mobile point-of-sale (MPOS) functionality, that is in the physical possession of a Merchant and deployed in or at the Merchant's premises, and which enables a Cardholder to use a Card or Access Device to effect a Transaction for the purchase of products or services sold by such Merchant; or
- A Bank Branch Terminal.

A POS Terminal must comply with the POS Terminal security and other applicable Standards.

Point-of-Sale (POS) Transaction

The sale of products or services by a Merchant to a Cardholder pursuant to acceptance of a Card by the Merchant, or a Manual Cash Disbursement Transaction. A POS Transaction conducted by a Merchant may be a Card-present Transaction taking place in a face-to-face environment or at an unattended POS Terminal, or a Card-not-present Transaction taking place in a non-face-to-face environment (for example, an e-commerce, mail order, phone order, or recurring payment Transaction).

Portfolio

All Cards issued bearing the same major industry identifier, BIN/IIN, and any additional digits that uniquely identify Cards for routing purposes.

Principal Customer, Principal

A Customer that participates directly in Card-based Activity using its assigned BINs/IINs and which may Sponsor one or more Affiliates.

Processed PTA Transaction

A PTA Transaction which is:

1. Initiated by or on behalf of the Originating Institution using the Corporation System in accordance with the Standards; and
2. Cleared, meaning the Originating Institution transferred the PTA Transaction data within the applicable time frame to the Corporation using the Corporation System, for the purpose of a transfer of funds using the Corporation System, and such PTA Transaction data is subsequently transferred by the Corporation to the Receiving Customer for such purpose.

Processed Transaction

A Transaction which is:

1. Authorized by the Issuer via the Interchange System, unless a properly processed offline Chip Transaction approval is obtained or no authorization is required, in accordance with the Standards; and
2. Cleared, meaning the Acquirer transferred the Transaction Data within the applicable presentment time frame to the Corporation via the Interchange System, for the purpose of

a transfer of funds via the Interchange System, and such Transaction Data is subsequently transferred by the Corporation to the Issuer for such purpose.

Processing of Personal Data

Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of such data, including any operation defined as "Processing" under applicable Privacy and Data Protection Law.

Program

A Customer's Card issuing program, Merchant acquiring program, ATM Terminal acquiring program, Digital Activity program, and/or a PTA Program in which a Customer, a Network Enablement Partner, or other entity approved by the Corporation is Participating.

Program Service

Any service described in the Standards that directly or indirectly supports a Program and regardless of whether the entity providing the service is registered as a Service Provider of one or more Customers. The Corporation has the sole right to determine whether a service is a Program Service.

PTA Account

A PTA Originating Account and/or a PTA Receiving Account.

PTA Account Number

The account number allocated to a PTA Account by a PTA Customer.

PTA Account Portfolio

All PTA Accounts issued by a PTA Customer.

PTA Agreement

The agreement between the Corporation and a PTA Customer granting the PTA Customer the right to Participate in a PTA Program, in accordance with the Standards.

PTA Customer

A Customer that Participates in a PTA Program pursuant to a PTA Agreement.

PTA Originating Account

The funding source of the Originating Account Holder, from where funds are acquired by the Originating Institution to initiate a PTA Transaction.

PTA Program

A type of Payment Transfer Activity that is identified in the applicable Standards as being a PTA Program, including the MoneySend Program, the Mastercard Merchant Presented QR Program, and the Mastercard Gaming and Gambling Payments Program.

PTA Receiving Account

The Account or, if applicable for a particular PTA Program (as set forth in the Standards for such PTA Program), the Non-Mastercard Receiving Account, held by a Receiving Account Holder and to which the Receiving Customer must ensure receipt of a PTA Transaction.

PTA Settlement Guarantee Covered Program

A PTA Settlement Obligation arising from a PTA Transaction conducted pursuant to a PTA Program that is identified in the applicable Standards as being a PTA Settlement Guarantee Covered Program.

PTA Settlement Obligation

A financial obligation of a Principal or Association PTA Customer to another Principal or Association PTA Customer arising from a PTA Transaction.

PTA Transaction

A financial transaction in which funds are transferred from an Originating Institution to a Receiving Customer on behalf of Account Holders pursuant to a PTA Program.

Quick Response (QR) Code

An ISO 18004-compliant encoding and visualization of data.

Receiving Account Holder

The Account Holder receiving the PTA Transaction.

Receiving Agent

A PTA Customer that Participates in Payment Transfer Activity as an agent for the purpose of receiving a PTA Transaction.

Receiving Customer

A Receiving Agent or a Receiving Institution.

Receiving Institution (RI)

A PTA Customer that Participates in Payment Transfer Activity as a receiver of PTA Transactions on behalf of a Receiving Account Holder.

Region

A geographic region as defined by the Corporation from time to time. Refer to Appendix A of the *Mastercard Rules* manual.

Remote Electronic Transaction

In the Europe Region, all types of Card-not-present Transactions (e-commerce Transactions, recurring payment Transactions, installment Transactions, Credential-on-File Transactions, in-app Transactions, and Transactions completed through a Digital Wallet). Mail order and

telephone order (MO/TO) Transactions and Transactions completed with anonymous prepaid Cards are excluded from this definition.

Rules

The Standards set forth in this manual.

Service Provider

A person that performs Program Service. The Corporation has the sole right to determine whether a person is or may be a Service Provider and if so, the category of Service Provider. A Service Provider is an agent of the Customer that receives or otherwise benefits from Program Service, whether directly or indirectly, performed by such Service Provider.

Settlement Obligation

A financial obligation of a Principal or Association Customer to another Principal or Association Customer arising from a Transaction.

Shared Deposit Transaction

A deposit to a savings Account or checking Account conducted at an ATM Terminal located in the U.S. Region, initiated with a Card issued by a U.S. Region Customer other than the Acquirer, and processed through the Mastercard® ATM Network.

Solicitation, Solicit

An application, advertisement, promotion, marketing communication, or the like distributed as printed materials, in electronic format (including but not limited to an email, website, mobile application, or social media platform), or both intended to solicit the enrollment of a person or entity as a Cardholder or Account Holder or as a Merchant. To "Solicit" means to use a Solicitation.

Special Issuer Program

Issuer Activity that the Corporation deems may be undertaken only with the express prior consent of the Corporation. As of the date of the publication of these Rules, Special Issuer Programs include Affinity Card Programs, Co-Brand Card Programs, and Prepaid Card Programs, and with respect to Mastercard Activity only, Brand Value Transaction and

proprietary account, Remote Transaction Mastercard Account, and secured Mastercard Card Programs.

Sponsored Digital Activity Entity

A wholly-owned subsidiary (or other affiliated entity as approved by the Corporation) of a Digital Activity Sponsoring Customer. The Sponsored Digital Activity Entity may be approved at the sole discretion of the Corporation to participate in Digital Activity pursuant to a Digital Activity Agreement or other agreement with the Corporation.

Sponsored Merchant

A merchant that, pursuant to an agreement with a Payment Facilitator, is authorized to accept Cards when properly presented. Sponsored Merchant is also referred to as Submerchant. Sponsored Merchant is also referred to as Submerchant.

Sponsored Merchant Agreement

An agreement between a Sponsored Merchant and a Payment Facilitator that sets forth the terms pursuant to which the Sponsored Merchant is authorized to accept Cards. Sponsored Merchant Agreement is also referred to as Submerchant Agreement.

Sponsor, Sponsorship

The relationship described in the Standards between

- a Principal or Association and an Affiliate that engages in Activity indirectly through the Principal or Association, in which case, the Principal or Association is the Sponsor of the Affiliate and the Affiliate is Sponsored by the Principal or Association;
- a Payment Facilitator and a Sponsored Merchant, in which case the Payment Facilitator is the Sponsor of the Sponsored Merchant and the Sponsored Merchant is Sponsored by the Payment Facilitator; or
- a Digital Activity Sponsoring Customer and a Sponsored Digital Activity Entity, in which case the Digital Activity Sponsoring Customer is the Sponsor of the Sponsored Digital Activity Entity.

"Sponsorship" means the Sponsoring of a Customer, a Sponsored Merchant, or a Sponsored Digital Activity Entity.

Staged Digital Wallet

Functionality that can be used at more than one retailer, and by which the Staged Digital Wallet Operator effects a two-stage payment to a retailer to complete a purchase initiated by a Cardholder. The following may occur in either order:

- **Payment stage**—In the payment stage, the Staged DWO pays the retailer by means of:
  - A proprietary non-Mastercard method (and not with a Mastercard Card); or
  - A funds transfer to an account held by the Staged DWO for or on behalf of the retailer.
- **Funding stage**—In the funding stage, the Staged DWO uses a Mastercard or Maestro Account provided to the Staged DWO by the Cardholder (herein, the "funding account") to perform a transaction that funds or reimburses the Staged Digital Wallet.

The retailer does not receive Mastercard or Maestro Account data or other information identifying the network brand and payment card issuer for the funding account.

Staged Digital Wallet Operator (DWO)

A registered Service Provider that operates a Staged Digital Wallet.

Standards

The organizational documents, operating rules, regulations, policies, and procedures of the Corporation, including but not limited to any manuals, guides, announcements or bulletins, as may be amended from time to time.

Stand-In Parameters

A set of authorization requirements established by the Corporation or the Issuer that are accessed by the Interchange System using the Stand-In Processing Service to determine the appropriate responses to authorization requests.

Stand-In Processing Service

A service offered by the Corporation in which the Interchange System authorizes or declines Transactions on behalf of and uses Stand-In Parameters provided by the Issuer (or in some cases, by the Corporation). The Stand-In Processing Service responds only when the Issuer is unavailable, the Transaction cannot be delivered to the Issuer, or the Issuer exceeds the response time parameters set by the Corporation.

Strong Customer Authentication (SCA)

Authentication as required by the 2nd Payment Services Directive (Directive [EU] 2015/2366 of 25 November 2015) Regulatory Technical Standards on Strong Customer Authentication (as amended and replaced from time to time).

Sub-licensee

A person authorized in writing to use a Mark either by a Licensee in accordance with the Standards or by the Corporation.

Terminal

Any attended or unattended device capable of the electronic capture and exchange of Account data that meets the Corporation requirements for Terminal eligibility, functionality, and security, and permits a Cardholder to effect a Transaction in accordance with the Standards. An ATM Terminal, Bank Branch Terminal, and POS Terminal is each a type of Terminal.

Third Party Processor (TPP)

A Service Provider that performs any one or more of the services as TPP Program Service.

Token

A numeric value that (i) is a surrogate for the primary account number (PAN) used by a payment card issuer to identify a payment card account or is a surrogate for the PTA Account Number used by a PTA Customer to identify a PTA Account; (ii) is issued in compliance with the EMV Payment Tokenization Specification Technical Framework; and (iii) passes the basic validation rules for a PAN, including the Luhn Formula for Computing Modulus 10 Check Digit. Also see Mastercard Token.

Token Aggregator

See On-behalf Token Requestor.

Tokenization, Tokenize

The process by which a Mastercard Token replaces an Account PAN or a PTA Account Number.

Token Requestor

An entity that requests the replacement of Account PANs with Mastercard Tokens.

Token Vault

A repository of tokens that are implemented by a tokenization system, which may also perform primary account number (PAN) mapping and cryptography validation.

Transaction

A financial transaction arising from the proper acceptance of a Card or Account bearing or identified with one or more of the Brand Marks, either alone or in combination with the marks of another payment scheme, at a Card acceptance location and identified in messages with a Card Program identifier.

Transaction Data

Any data and/or data element or subelement that the Standards and/or the Corporation's interface specifications require to be used to initiate, authorize, clear, and/or settle a Transaction or PTA Transaction (whether authorized, cleared, and/or settled using the Interchange System or otherwise) or that the Corporation requires to be provided.

Virtual Account

A Mastercard Account issued without a physical Card or Access Device. A Virtual Account cannot be electronically read.

Volume

The aggregate financial value of a group of Transactions. "Volume" does not mean the number of Transactions.

Wallet Token Requestor

A Wallet Token Requestor is a Pass-through DWO that connects directly to the Mastercard Digital Enablement Service (MDES) for the purpose of Tokenizing a Mastercard or Maestro

Account primary account number (PAN) provided by a Cardholder for use in a future Transaction.

Word Mark

A Mark consisting of the name of one of the Corporation's brands followed by a registered trademark ®or ™symbol (depending on its trademark status in a particular country) or the local law equivalent. See Cirrus Word Mark, Maestro Word Mark, Mastercard Word Mark.

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Information Available Online

Mastercard provides details about the standards used for this document, including times expressed, language use, and contact information, on the Technical Resource Center (TRC). Go to the Rules collection of the References section for centralized information.