Security Rules and Procedures

Merchant Edition

1 August 2023

SPME

Contents

Chapter 1 Customer Obligations

This chapter describes general Customer compliance and Program obligations relating to Mastercard Card issuing and Merchant acquiring Program Activities.

1.1 Compliance with the Standards

This manual contains Standards. Each Customer must comply fully with these Standards.

All of the Standards in this manual are assigned to noncompliance category A under the compliance framework set forth in Chapter 2 of the *Mastercard Rules* manual ("the compliance framework"), unless otherwise specified in the table below. The noncompliance assessment schedule provided in the compliance framework pertains to any Standard in the *Security Rules and Procedures* manual that does not have an established compliance Program. The Corporation may deviate from the schedule at any time.

Section Number	Section Title	Category
1.3	The Security Contact	C
7.1.2	Retention of Investigative Records	C

1.2 Conflict with Law

A Customer is excused from compliance with a Standard in any country or region of a country only to the extent that compliance would cause the Customer to violate local applicable law or regulation, and further provided that the Customer promptly notifies the Corporation, in writing, of the basis for and nature of an inability to comply. The Corporation has the authority to approve local alternatives to these Standards.

1.3 The Security Contact

Each Customer must have a Security Contact listed for each of its Member IDs/ICA numbers in the Company Contact Management application on Mastercard Connect™.

1.4 Connecting to Mastercard—Physical and Logical Security Requirements

Each Customer and any agent thereof must be able to demonstrate to the satisfaction of Mastercard the existence and use of meaningful physical and logical security controls for any communications processor or other device used to connect the Customer's processing systems to the Mastercard Network (herein, "a Mastercard Network Device") and all associated components, including all hardware, software, systems, and documentation (herein collectively

referred to as "Service Delivery Point Equipment") located on-site at the Customer or agent facility. Front-end communications processors include Mastercard interface processors (MIPs), network interface units (NIUs), and debit interface units (DIUs).

The controls must meet the minimum requirements described in this section, and preferably will include the recommended additional parameters.

1.4.1 Minimum Security Requirements

At a minimum, the Customer or its agent must put in place the following controls at each facility housing Service Delivery Point Equipment:

1. Each network segment connecting a Mastercard Network Device to the Customer's processing systems must be controlled tightly, as appropriate or necessary to prevent unauthorized access to or from other public or private network segments.
2. The connectivity provided by each such network segment must be dedicated wholly and restricted solely to the support of communications between Mastercard and the Customer's processing systems.
3. The Customer or its agent must replace each vendor-supplied or default password present on the Customer's processing systems, each Mastercard Network Device, and any device providing connectivity between them with a "strong password." A strong password contains at least eight characters, uses a combination of letters, numbers, symbols, punctuation, or all, and does not include a name or common word(s).
4. The Customer or its agent must conduct regular periodic reviews of all systems and devices that store Account information to ensure that access is strictly limited to appropriate Customer personnel on a "need to know" basis.
5. The Customer or its agent must notify Mastercard within 30 business days of any change in the personnel designated to administer the Mastercard Network Device. Refer to Appendix B of this manual for contact information.
6. The Customer or its agent must maintain and document appropriate audit procedures for each Mastercard Network Device. Audit reports must be maintained and accessible to the Customer for at least one year, including a minimum of 90 days in an easily retrieved electronic format.
7. The Customer must ensure that the software employed in any system or device used to provide connectivity to the Mastercard Network is updated with all appropriate security patches, revisions, and other updates as soon after a release as is practicable.
8. The physical location of the Service Delivery Point Equipment must be accessible only by authorized personnel of the Customer or its agent. Visitor access must be controlled by at least one of the following measures:
    a. Require each visitor to provide government-issued photo identification before entering the physical location; and/or
    b. Require each visitor to be escorted to the physical location by authorized personnel of the Customer or its agent.
9. If the physical location of the Service Delivery Point Equipment provides common access to other devices or equipment, then the Mastercard Network Device must be stored in a

cabinet that is locked both in front and the rear at all times. Keys to the cabinet must be stored in a secured location.

10. The Customer or its agent must have documented procedures for the removal of Service Delivery Point Equipment from the physical location.

1.4.2 Additional Recommended Security Requirements

Customers and their agents are strongly encouraged to put in place the following additional controls at each facility housing a Mastercard Network Device:

1. Placement of the Mastercard Network Device in a physical location that is enclosed by floor-to-ceiling walls.
2. Continual monitoring of the Mastercard Network Device by cameras or other type of electronic surveillance system. Video records should be maintained for a minimum of 90 days.

1.4.3 Ownership of Service Delivery Point Equipment

Effective as of date of placement, the Customer is granted a non-exclusive, non-assignable license to use the Service Delivery Point Equipment owned or controlled by Mastercard. The Customer may not take any action adverse to the interests of Mastercard with respect to the use of the Service Delivery Point Equipment.

The Customer at all times remains responsible for the safety and proper use of all Service Delivery Point Equipment placed at a location by request of the Customer, and must employ at that location the minimum security requirements set forth in this section 1.4. At its own expense, the Customer must promptly return all Service Delivery Point Equipment owned or controlled by Mastercard to Mastercard upon request of Mastercard and without such request, in the event of bankruptcy or insolvency.

1.4.4 Component Authentication

All components actively participating in the Interchange System must authenticate each other by means of cryptographic procedures, either explicitly by a specific authentication protocol or implicitly by correct execution of a cryptographic service possessing secret information (for example, the shared key or the logon ID).

A component actively participates in the Interchange System if, because of its position in the system, it can evaluate, modify, or process security-related information.

1.5 Data Protection

In addition to Rule 3.13 of the *Mastercard Rules*, the Corporation and each Customer must comply with (1) Applicable Data Protection Law and (2) Appendix D (Covered Programs Privacy and Data Protection Standards), in each case when Processing Personal Data in the context of Activity related to Account Data Compromise events, Mastercard Alert to Control High-risk

(Merchants) (MATCH™) system, the Excessive Chargeback Program, the Merchant Registration Program, and the Franchise Management Program (collectively a "Covered Program").

1.5.1 Compliance with Privacy, Data Protection and Information Security Requirements

The Corporation and each Customer must comply with Applicable Data Protection Law when Processing Personal Data in the context of Activity related to a Covered Program.

Chapter 2 Cybersecurity Standards and Programs

This chapter is relevant to all Customers, Merchants, Service Providers, and any other Customer agents that store, process, or transmit Account, Card, Cardholder, or Transaction data.

2.1 Cybersecurity Standards

Each Customer and any agent thereof is expected to establish and maintain meaningful cybersecurity controls for any environment, system, or device used to store or process Confidential Information or Account Data, whether temporarily or permanently and whether directly or indirectly.

For purposes of this Chapter 2:

- "Confidential Information" means any information of any nature resulting from Activity, Digital Activity, Payment Transfer 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
- "Account Data" means any Cardholder Data and/or Sensitive Authentication Data, where these terms have the meanings set forth in the *Payment Card Industry (PCI) Data Security Standard* and in this section, and include, by way of example and not limitation:
  - Cardholder Data—The Cardholder name, primary account number (PAN), and expiration date associated with an Account (including any Token or Virtual Account) and, the service code on a magnetic stripe Card, and
  - Sensitive Authentication Data—The full contents of a Card's magnetic stripe, Card validation code 2 (CVC 2) data, and PIN or PIN block data.

Cybersecurity Minimum Requirement

Each Customer must ensure that any Customer environment that stores, processes, or transmits Account Data complies with the *PCI Data Security Standard*, in accordance with the Mastercard Site Data Protection (SDP) Program, all other applicable PCI Security Standards (as listed in section 2.1.1), and the Mastercard cybersecurity programs described in Chapter 2 of this manual.

NOTE: Additions to this Rule appear in the "Asia/Pacific Region" section at the end of this chapter.

Cybersecurity Best Practice

As a best practice to ensure sufficient cybersecurity controls are established and maintained, all Customer environments, systems, or devices used to store, process, or transmit Confidential Information are recommended to comply with at least one of the following:

- The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF); or
- One of the standards included as "Informative References" to the NIST CSF, currently:
  - Control Objectives for Information and Related Technology (COBIT)
  - Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense (CIS Controls)
  - American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001
- NIST Special Publication (SP) 800-53 Rev. 4 - NIST SP 800-53

The following cybersecurity standards documents:	May be found at:
PCI Security Standards, including all of the documents listed in section 2.1.1	https://www.pcisecuritystandards.org
NIST CSF and NIST CSF "Informative References"	https://www.nist.gov/cyberframework

NOTE: Additions to this Rule appear in the "Asia/Pacific Region" section at the end of this chapter.

2.1.1 Payment Card Industry (PCI) Security Standards

PCI Security Standards are technical and operational requirements established by the Payment Card Industry Security Standards Council (PCI SSC) to act as a minimum baseline to protect Account data. Mastercard requires that all Customers, Merchants, Service Providers, and other Customer agents that store, process, or transmit Card, Cardholder, or Transaction data adhere to the most current PCI Security Standards.

Mastercard recommends that entities required to employ a PCI SSC assessor for PCI compliance validation rotate individual PCI SSC assessors engaged from within independent security organizations, as a best practice.

The following table describes the PCI Security Standards and compliance requirements applicable to Issuers, Acquirers, Merchants, Service Providers, Card production vendors, and other Customer agents. All of the PCI Security Standards documents referenced in Table 2.1 are available on the PCI SSC website at www.pcisecuritystandards.org.

Table 2.1—PCI Security Standards Documentation and Compliance Requirements and Recommendations

PCI Security Standard	Compliance Requirements and Recommendations
PCI Data Security Standard ("PCI DSS")	Compliance is strongly recommended for all Issuers, Acquirers, Merchants, Service Providers, and any other person or entity that a Customer permits, directly or indirectly, to store, transmit, or process Account data. Validation of compliance is required for Level 1, 2, and 3 Merchants and all Service Providers under the Mastercard Site Data Protection (SDP) Program (refer to section 2.2 for more information).

PCI Security Standard	Compliance Requirements and Recommendations
PCI Payment Application Data Security Standard ("PCI PA-DSS")	Compliance is required for all Merchants and Service Providers that use eligible third party-provided payment applications, unless the payment application is compliant with the *PCI Secure Software Standard*. Refer to the *PCI PA-DSS Program Guide* for information about the applicability of the PCI PA-DSS to third party-provided payment applications. Refer to the *PCI QIR Program Guide* for information about the applicability of Qualified Integrator & Reseller (QIR) engagement for third party-provided payment application implementation. Use of a QIR listed on the PCI SSC website is strongly recommended.
PCI Token Service Providers—Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) ("PCI TSP Security Requirements")	Compliance is strongly recommended for any Issuer that performs Token Service Provider (TSP) services on its own behalf, and any entity that performs or proposes to perform TSP Program Service as the TSP of a Customer. Refer to Chapter 7 of the *Mastercard Rules* for more information about third-party TSP requirements.
PCI 3-D Secure—Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: Access Control Server (ACS), Directory Server (DS), and 3DS Server (3DSS) ("PCI 3DS Core Security Standard")	Compliance is required for any Service Provider that performs or provides 3-D Secure (3DS) functions as defined in the *EMV 3-D Secure Protocol and Core Functions Specification*. Validation of compliance is required for such Service Providers under the Mastercard SDP Program (refer to section 2.2). Compliance is strongly recommended for any Merchant that performs or provides 3DS functions as defined in the *EMV 3-D Secure Protocol and Core Functions Specification*. Refer to Chapter 7 of the *Mastercard Rules* for more information about 3DS Service Provider requirements.

PCI Security Standard	Compliance Requirements and Recommendations
PCI 3-D Secure—Security Requirements and Assessment Procedures for EMV 3-D Secure SDK ("PCI 3DS SDK Security Standard")	Compliance is required for any Service Provider that uses 3DS Software Development Kits (SDKs). Use of approved 3DS SDKs is strongly recommended for any Merchant that performs or provides 3DS functions as defined in the *EMV 3-D Secure Protocol and Core Functions Specification*. Approved 3DS SDKs are listed on the PCI SSC website at www.pcisecuritystandards.org.
PCI Point-to-Point Encryption: Solution Requirements and Testing Procedures	Compliance is required for eligible Merchants participating in the Mastercard PCI DSS Compliance Validation Exemption Program and implementing a Point-to-Point Encryption (P2PE) solution (refer to section 2.2.4 for more information).
PCI Card Production & Provisioning Physical Security Requirements *PCI Card Production & Provisioning Logical Security Requirements*	Compliance is required for any Card production vendor, pursuant to the Global Vendor Certification Program (GVCP), and any Issuer that performs Card production activities on its own behalf (refer to section 2.3 and Appendix C for more information).
PCI PIN Security Requirements *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements* *PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Security Requirements* *PCI PIN Transaction Security (PTS) Device Testing and Approval Program Guide and PCI Approved PTS Devices* list *PCI Software-based PIN Entry on COTS (SPoC)™ Security Requirements* *PCI Mobile Payments on COTS (MPoC™) Security and Test Requirements*	Compliance is required for all Customers and their agents performing PIN encipherment or any other aspect of PIN processing involving PIN entry by means of a: • PIN entry device (PED) or encrypting PIN pad (EPP) on a Terminal (including a Mobile Point-of-Sale [MPOS] Terminal); or • Application (App) running on a Commercial Off-The-Shelf (COTS) device that is part of either a PCI approved (SPoC Solution) or a PCI approved MPoC Solution. Refer to section 2.4 for more information; also see Chapter 4 for additional PIN-related requirements.
PCI Forensic Investigator Program Guide ("*PFI Program Guide*")	Compliance is required for any Acquirer that engages the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation in order to assess the cause, scope, magnitude, duration, and effects of an ADC Event or Potential ADC Event.

PCI Security Standard	Compliance Requirements and Recommendations
PCI Software Security Framework (SSF)—PCI Secure Software Requirements and Assessment Procedures ("PCI Secure Software Standard")	Compliance is required for all Merchants and Service Providers that use eligible third party-provided payment software. Refer to the *PCI Secure Software Program Guide* for information about the applicability of the PCI Secure Software Standard to third party-provided payment software.
PCI Software Security Framework (SSF)—PCI Secure Software Lifecycle (Secure SLC) Requirements and Assessment Procedures ("PCI Secure SLC Standard")	Compliance is strongly recommended for any Merchant or Service Provider that uses third party-provided payment software.

2.2 Mastercard Site Data Protection (SDP) Program

NOTE: This section applies to Mastercard and Maestro Transactions.

The Mastercard Site Data Protection (SDP) Program consists of Rules, guidelines, best practices, and approved compliance validation tools to foster broad compliance with the PCI Security Standards. The SDP Program is designed to help Customers, Merchants, and Service Providers (Third Party Processors [TPPs], Data Storage Entities [DSEs], Payment Facilitators [PFs], Staged Digital Wallet Operators [SDWOs], Digital Activity Service Providers [DASPs], Token Service Providers [TSPs], Terminal Servicers [TSs], AML/Sanctions Service Providers, 3-D Secure Service Providers [3-DSSPs], Installment Service Providers [ISPs]), and Merchant Payment Gateways [MPGs]) protect against Account Data Compromise (ADC) Events.

NOTE: For the purposes of the SDP Program, TPPs, DSEs, PFs, SDWOs, DASPs, TSPs, TSs, AML/Sanctions Service Providers, 3-DSSPs, ISPs, and MPGs are collectively referred to as "Service Providers" in this chapter. Refer to section 10.1 of this manual for the definitions of an Account Data Compromise Event and a Potential Account Data Compromise Event.

Compliance with the *Payment Card Industry Data Security Standard* (PCI DSS) and all other applicable PCI Security Standards is required for all Issuers, Acquirers, Merchants, Service Providers, and any other person or entity that a Customer permits, directly or indirectly, to store, transmit, or process Account Data. Only Merchants and Service Providers must validate their compliance to Mastercard, as set forth in sections 2.2.2 and 2.2.3 respectively, in order to be deemed compliant with the Mastercard SDP Program.

Mastercard has sole discretion to interpret and enforce the SDP Program Standards.

2.2.1 Customer Compliance Requirements

Compliance with the PCI DSS is required for all Issuers and Acquirers, although validation of the Customer's compliance is not required.

To ensure compliance with the Mastercard SDP Program, an **Issuer** must:

- Communicate the SDP Program requirements to each Level 1 and Level 2 Service Provider, and validate the Service Provider's compliance with the PCI DSS and any other applicable PCI Security Standard by reviewing the *Payment Card Industry Self-Assessment Questionnaire* (SAQ) or the Report on Compliance (ROC).
- Submit the annual PCI compliance validation (the PCI Attestation of Compliance [AOC]) for each Level 1 and Level 2 Service Provider by email message to pcireports@mastercard.com, after initial registration with Mastercard and every year thereafter. If a newly registered Service Provider is not yet compliant, the PCI Action Plan available on the Service Provider page of the SDP Program website must be completed and submitted for review.

To ensure compliance with the Mastercard SDP Program, an **Acquirer** must:

- Communicate the SDP Program requirements to each Level 1, Level 2, and Level 3 Merchant, and validate the Merchant's compliance with the PCI DSS by reviewing the *Payment Card Industry Self-Assessment Questionnaire* or the ROC.
- Submit the SDP Acquirer Submission and Compliance Status Form available on the Acquirer page of the SDP Program website, for each Level 1, Level 2, and Level 3 Merchant semi-annually by email message to sdp@mastercard.com.

For this reporting period...	Submit the form(s) no later than...
1 October to 31 March	31 March
1 April to 30 September	30 September

- Validate to Mastercard that the Acquirer has a risk management program in place to identify and manage payment security risk within the Acquirer's Level 4 Merchant portfolio.
- Communicate the SDP Program requirements to each Level 1 and Level 2 Service Provider, and validate the Service Provider's compliance with the PCI DSS and any other applicable PCI Security Standard by reviewing the *Payment Card Industry Self-assessment Questionnaire* and the ROC.
- Submit annual PCI validation (the PCI Attestation of Compliance [AOC]) for each Level 1 and Level 2 Service Provider by email message to pcireports@mastercard.com after initial registration with Mastercard and every year thereafter. If a newly registered Service Provider is not yet compliant, the PCI Action Plan available on the Service Provider page of the SDP Program website must be completed and submitted for review.

A Customer that complies with the SDP Program requirements may qualify for a reduction, partial or total, of certain costs or assessments if the Customer is impacted by an ADC Event, whether caused by the Customer itself, a Merchant, or a Service Provider.

2.2.2 Merchant Compliance Requirements

This section describes Level 1, Level 2, Level 3 and Level 4 Merchant criteria and how a Merchant may successfully validate compliance with the PCI DSS and all other applicable PCI Security Standards and apply cybersecurity best practices. Refer to section 2.2.4 regarding alternative

means by which a Merchant may validate PCI DSS compliance if implementing secure technologies.

The Acquirer must ensure, with respect to each of its Merchants, that "transition" from one PCI level to another (for example, the Merchant transitions from Level 4 to Level 3 due to Transaction volume increases), that such Merchant achieves compliance with the requirements of the applicable PCI level as soon as practical, but in any event not later than one year after the date of the event that results in or causes the Merchant to transition from one PCI level to another.

All Level 1, Level 2, and Level 3 Merchants that use any third party-provided payment applications or payment software must validate that each payment application or payment software used is listed on the PCI Security Standards Council (SSC) website at www.pcisecuritystandards.org as compliant with either the *Payment Card Industry Payment Application Data Security Standard* (PCI PA-DSS) or the PCI Secure Software Standard, as applicable. Mastercard recommends that Merchants use a Qualified Integrator & Reseller (QIR) listed on the PCI SSC website to implement a PCI PA-DSS-compliant payment application, as applicable.

Mastercard recommends that Merchants using third party-provided payment software ensure the payment software vendor complies with the PCI Secure SLC Standard.

Mastercard recommends that any Merchant that performs or provides 3-D Secure (3DS) functions as defined in the *EMV 3-D Secure Protocol and Core Functions Specification* comply with the *PCI 3DS Core Security Standard* and use approved 3DS Software Development Kits (SDKs) listed on the PCI SSC website, as applicable.

Level 1 Merchants

A Merchant that meets any one or more of the following criteria is deemed to be a Level 1 Merchant and must validate compliance with the PCI DSS:

- Any Merchant having greater than six million total combined Mastercard and Maestro Transactions annually,
- Any Merchant meeting the Level 1 criteria of Visa, and
- Any Merchant that Mastercard, in its sole discretion, determines should meet the Level 1 Merchant requirements to minimize risk to the system, which may include any Merchant that has a confirmed ADC Event.

To validate compliance, each Level 1 Merchant must successfully undergo an annual PCI DSS assessment resulting in the completion of a ROC conducted by a PCI SSC-approved Qualified Security Assessor (QSA) or PCI SSC-certified Internal Security Assessor (ISA).

Level 2 Merchants

Unless deemed to be a Level 1 Merchant, the following are deemed to be a Level 2 Merchant and must validate compliance with the PCI DSS:

- Any Merchant with greater than one million but less than or equal to six million total combined Mastercard and Maestro Transactions annually, and
- Any Merchant meeting the Level 2 criteria of Visa.

To validate compliance, each Level 2 Merchant must successfully complete an annual SAQ. Level 2 Merchants completing SAQ A, SAQ A-EP or SAQ D must additionally engage a PCI SSC-approved QSA or PCI SSC-certified ISA for compliance validation.

Level 2 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA or PCI SSC-certified ISA to complete a ROC instead of performing an SAQ.

Level 3 Merchants

Unless deemed to be a Level 1 or Level 2 Merchant, the following are deemed to be a Level 3 Merchant and must validate compliance with the PCI DSS:

- Any Merchant with greater than 20,000 but less than or equal to one million total combined Mastercard and Maestro electronic commerce (e-commerce) Transactions annually, and
- Any Merchant meeting the Level 3 criteria of Visa.

To validate compliance, each Level 3 Merchant must successfully complete an annual SAQ.

Level 3 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA to complete a ROC instead of performing an SAQ.

Level 4 Merchants

Any Merchant not deemed to be a Level 1, Level 2, or Level 3 Merchant is deemed to be a Level 4 Merchant. Compliance with the PCI DSS is required for a Level 4 Merchant, although validation of compliance is optional for a Level 4 Merchant. However, a validation of compliance is strongly recommended for Acquirers with respect to each Level 4 Merchant in order to reduce the risk of an ADC Event and for an Acquirer potentially to gain a partial waiver of related assessments.

A Level 4 Merchant may validate compliance with the PCI DSS by successfully completing an annual SAQ.

Level 4 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA to complete a ROC instead of performing an SAQ.

2.2.3 Service Provider Compliance Requirements

This section describes Level 1 and Level 2 Service Provider criteria, and how a Service Provider may successfully validate compliance with the PCI DSS and all other applicable PCI Security Standards and apply cybersecurity best practices.

Mastercard recommends that each Level 1 and Level 2 Service Provider demonstrates to Mastercard its compliance with the Designated Entities Supplemental Validation (DESV) appendix of the PCI DSS.

All Level 1 and Level 2 Service Providers that use any third party-provided payment applications or payment software must validate that each payment application or payment software used is listed on the PCI SSC website at www.pcisecuritystandards.org as compliant with either the PCI PA-DSS DSS or the PCI Secure Software Standard, as applicable.

Mastercard recommends that Service Providers using third party-provided payment software ensure the payment software vendor complies with the PCI Secure SLC Standard.

Compliance with the *PCI 3DS Core Security Standard* is required for any Service Provider that performs or provides 3DS functions as defined in the *EMV 3-D Secure Protocol and Core Functions Specification*. All Service Providers that use any 3DS SDK must validate that each 3DS SDK used is listed on the PCI SSC website at www.pcisecuritystandards.org as compliant with the *PCI 3DS SDK Security Standard*, as applicable.

Level 1 Service Providers

A Level 1 Service Provider is any TPP, MPG, SDWO, DASP, TSP, AML/Sanctions Service Provider, 3-DSSP, or ISP (regardless of volume); and any DSE or PF that stores, transmits, or processes more than 300,000 total combined Mastercard and Maestro Transactions annually.

Each Level 1 Service Provider must validate compliance with the PCI DSS, and each 3-DSSP must validate compliance with the *PCI 3DS Core Security Standard* by successfully undergoing an annual PCI assessment resulting in the completion of a ROC conducted by an appropriate PCI SSC-approved QSA.

Level 2 Service Providers

A Level 2 Service Provider is any DSE or PF that is not deemed a Level 1 Service Provider and that stores, transmits, or processes 300,000 or less total combined Mastercard and Maestro Transactions annually; and any TS.

Each Level 2 Service Provider must validate compliance with the PCI DSS by successfully completing an annual SAQ.

As an alternative to validating compliance with the PCI DSS, a DSE qualifying as a Level 2 Service Provider may submit a PCI PIN Security Requirements Attestation of Compliance for Onsite Assessments from a PCI SSC-approved Qualified PIN Assessor (QPA) every two years to the Mastercard SDP Department, provided that the DSE does not perform services involving the storage, transmission, or processing of Account, Cardholder, or Transaction Data.

As an alternative to validating compliance with the PCI DSS, a TS may submit a completed Terminal Servicer QIR Participation Validation Form to the Mastercard SDP Department, provided that the TS **does not** perform services involving the storage, transmission, or processing of Account, Cardholder, or Transaction Data, but the TS has access to such Data within the Cardholder Data Environment (CDE) (as the term is defined by the PCI SSC). The Terminal Servicer QIR Participation Validation Form is available on the Service Provider page of the SDP Program website.

NOTE: Service Provider classifications (TPPs, DSEs, PFs, SDWOs, DASPs, TSPs, TSs, AML/Sanctions Service Providers, 3-DSSPs, ISPs, and MPGs) are determined by Mastercard. Service Provider registrations with Mastercard will not be deemed complete until the Service Provider's compliance with the SDP Program is validated. Refer to Chapter 7 of the *Mastercard Rules* manual for additional Service Provider registration requirements.

2.2.4 Mastercard Cybersecurity Incentive Program (CSIP)

The Mastercard Cybersecurity Incentive Program (CSIP) provides eligible Merchants using secure technologies such as EMV chip technology, a PCI-listed point-to-point encryption (P2PE)

solution, or EMV payment tokenization increased flexibility within the SDP Standards. The CSIP is a component of the SDP Program and is optional for Merchants. The CSIP incentivizes Merchant participation by either reducing PCI compliance validation requirements or by eliminating the requirement to annually validate compliance with the PCI DSS.

Mastercard PCI DSS Risk-based Approach

A qualifying Level 1 or Level 2 Merchant located outside of the U.S. Region may use the Mastercard PCI DSS Risk-based Approach, which reduces a Merchant's compliance requirements to validating compliance with the first two of the six total milestones set forth in the *PCI DSS Prioritized Approach*, as follows:

- A Level 1 Merchant must validate compliance through a PCI DSS assessment resulting in the completion of a ROC conducted by a PCI SSC-approved QSA or PCI SSC-certified ISA;
- A Level 2 Merchant must validate compliance through an SAQ. Level 2 Merchants completing SAQ A, SAQ A-EP or SAQ D must additionally engage a PCI SSC-approved QSA or PCI SSC-certified ISA for compliance validation; and
- Each Level 1 and Level 2 Merchant must annually re-validate compliance with milestones one and two using an SAQ.

To qualify as compliant with the Mastercard PCI DSS Risk-based Approach, a Merchant must satisfy all of the following:

- The Merchant must certify that it is not storing Sensitive Authentication Data.
- On a continuous basis, the Merchant must keep fully segregated the "Card-not-present" Transaction environment from the "face-to-face" Transaction environment. A face-to-face Transaction requires the Card, the Cardholder, and the Merchant to all be present together at the time and place of the Transaction.
- For a Merchant located in the Europe Region, at least 95 percent of the Merchant's annual total count of Card-present Mastercard and Maestro Transactions must occur at Hybrid POS Terminals.
- For a Merchant located in the Asia/Pacific Region, Canada Region, Latin America and the Caribbean Region, or Middle East/Africa Region, at least 75 percent of the Merchant's annual total count of Card-present Mastercard and Maestro Transactions must occur at Hybrid POS Terminals.
- The Merchant must not have experienced an ADC Event or Potential ADC Event within the last 3 years, including but not limited to outstanding liabilities or actions preventing complete closure of ADC Event. At the discretion of Mastercard, this and other criteria may be waived if the Merchant validated full PCI DSS compliance at the time of the ADC Event or Potential ADC Event.
- The Merchant must establish and annually test an ADC Event incident response plan.

Information about the *PCI DSS Prioritized Approach* is available at:

https://www.pcisecuritystandards.org/document_library

Mastercard PCI DSS Compliance Validation Exemption Program

All qualifying Merchants may participate in the Mastercard PCI DSS Compliance Validation Exemption Program (Exemption Program), which exempts the Merchant from annually validating its compliance with the PCI DSS.

To qualify or remain qualified to participate in the Exemption Program, a duly authorized and empowered officer of the Merchant must certify to the Merchant's Acquirer in writing that the Merchant has satisfied all of the following:

1. The Merchant does not store Sensitive Authentication Data. The Acquirer must notify Mastercard through compliance validation reporting of the status of Merchant storage of Sensitive Authentication Data;
2. The Merchant has not been identified by Mastercard as having experienced an ADC Event or Potential ADC Event during the prior three years, including but not limited to outstanding liabilities or actions preventing complete closure of ADC Event;
3. The Merchant has established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements; and
4. The Merchant has satisfied one of the following:
    a. At least 75 percent of the Merchant's annual total acquired Mastercard and Maestro Transaction count is processed through Hybrid POS Terminals, as determined based on the Merchant's transactions processed during the previous twelve (12) months through the Global Clearing Management System (GCMS) and/or Single Message System. Transactions that were not processed by Mastercard may be included in the annual acquired Transaction count if the data is readily available to Mastercard;
    b. The Merchant has implemented a P2PE solution listed on the PCI SSC website; **OR**
    c. At least 75 percent of the Merchant's annual total acquired Mastercard and Maestro Transaction count is processed using Mastercard Tokens from TSPs compliant with the Token Service Provider Standards.

As a best practice, qualifying Merchants participating in the Exemption Program are recommended to validate compliance with the PCI DSS within the previous twelve (12) months of entering the Exemption Program.

An Acquirer must retain all Merchant certifications of eligibility for the Exemption Program for a minimum of five (5) years. Upon request by Mastercard, the Acquirer must provide a Merchant's certification of eligibility for the Exemption Program and any documentation and/or other information applicable to such certification. An Acquirer is responsible for ensuring that each Exemption Program certification is truthful and accurate.

A Merchant that does not satisfy the Exemption Program's eligibility criteria, including any Merchant whose Transaction volume is primarily from e-commerce that does not utilize EMV Payment Tokenization and Mail Order/Telephone Order (MO/TO) acceptance channels, must continue to validate its PCI DSS compliance in accordance with section 2.2.2.

All Merchants must maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation is a requirement.

2.2.5 SDP Program Noncompliance Assessments

Mastercard has the right to audit Customer compliance with the SDP Program requirements. Noncompliance on or after the required implementation date may result in assessments described in Table 2.2.

Table 2.2—Assessments for Noncompliance with the SDP Program

Failure of the following to comply with the SDP Program mandate...	May result in an assessment of...
Classification	**Violations per calendar year**
Level 1 and Level 2 Merchants	Up to USD 25,000 for the first violation
	Up to USD 50,000 for the second violation
	Up to USD 100,000 for the third violation
	Up to USD 200,000 for the fourth violation
Level 3 Merchants	Up to USD 10,000 for the first violation
	Up to USD 20,000 for the second violation
	Up to USD 40,000 for the third violation
	Up to USD 80,000 for the fourth violation
Level 1 and Level 2 Service Providers	Up to USD 25,000 for the first violation
	Up to USD 50,000 for the second violation
	Up to USD 100,000 for the third violation
	Up to USD 200,000 for the fourth violation

Noncompliance also may result in Merchant termination; deregistration of a TPP, DSE, PF, SDWO, DASP, TSP, TS, AML/Sanctions Service Provider, 3-DSSP, ISP, or MPG as a Service Provider; delisting of a Service Provider from *The Mastercard SDP Compliant Registered Service Provider List*; or termination of the Issuer or Acquirer as a Customer as provided in Rule 2.1.2 of the *Mastercard Rules* manual.

Late SDP Acquirer Submission and Compliance Status Forms for semi-annual merchant compliance reporting submissions or failure to submit the required form(s) may result in an additional assessment to the Customer as described for Category A violations in Rule 2.1.4 of the *Mastercard Rules* manual.

2.2.6 Mandatory Compliance Requirements for Compromised Entities

Under the audit requirement set forth in section 10.3.1, the Acquirer must ensure that a detailed forensic investigation is conducted.

At the conclusion of the forensic investigation, Mastercard will provide a Mastercard Site Data Protection (SDP) Account Data Compromise Information Form for completion by the compromised entity itself, if the compromised entity is a Service Provider, or by its Acquirer, if the compromised entity is a Merchant. The form must be returned by email message to pci_adc@mastercard.com within 30 calendar days of its receipt, and must include:

- The names of the forensic investigator, QSA and the Approved Scanning Vendor (ASV);
- The entity's current level of compliance; and
- A gap analysis providing detailed steps required for the entity to achieve full compliance.

PCI DSS Compliance

As soon as practical, but no later than the PCI DSS compliance deadline shown in Table 2.3, the compromised entity or its Acquirer must provide evidence of compliance to Mastercard that the compromised entity has achieved full compliance with the PCI DSS.

Table 2.3 PCI DSS Compliance Deadlines and Evidence of Compliance for Compromised Entities

Classification	PCI DSS Compliance deadline from the Conclusion of the Forensic Investigation	Evidence of Compliance
Service Providers	90 calendar days	Both of the following: • PCI DSS ROC AOC conducted by a PCI SSC-approved QSA; and • DESV Supplemental ROC (S-ROC) AOC conducted by a PCI SSC-approved QSA within twelve (12) months from achieving full compliance with the PCI DSS
Level 1 or Level 2 Merchants	180 calendar days	PCI DSS ROC AOC conducted by a PCI SSC-approved QSA
Level 3 or Level 4 Merchants	180 calendar days	Either of the following: • PCI DSS ROC AOC conducted by a PCI SSC-approved QSA; or • PCI DSS SAQ AOC

Evidence of compliance for compromised entities must be submitted to Mastercard by email message to pci_adc@mastercard.com no later than the PCI DSS compliance deadline shown in Table 2.3.

Failure to comply with these requirements may result in SDP noncompliance assessments as described in section 2.2.5. Extension requests for compromised entities that do not meet the PCI DSS compliance deadline shown in Table 2.3 will not be approved by Mastercard.

Merchants

Any Merchant that has a confirmed ADC Event may be automatically reclassified to become a Level 1 Merchant. All compliance validation requirements and associated SDP noncompliance assessments for Level 1 Merchants will apply.

Service Providers

Any Service Provider that has a confirmed ADC Event, adverse inference (see section 10.3), and/or noncompliance for failure to cooperate in an ADC Event or forensic investigation will be automatically reclassified to become a Level 1 Service Provider.

In addition, a Service Provider's noncompliance will result in the automatic delisting from The Mastercard SDP Compliant Registered Service Provider List. A registered Service Provider may be placed back on the list only after the entity has re-validated compliance with the PCI DSS and has additionally demonstrated compliance with the DESV appendix of the PCI DSS within twelve (12) months from achieving full compliance with the PCI DSS as shown in Table 2.3.

2.3 Card Production Security Standards

As used in this section, and unless otherwise specified, the term "Card production" is applicable with respect to Cards and other types of Access Devices, including Contactless Payment Devices and Mobile Payment Devices.

An Issuer must ensure that all Card production activities are performed in compliance with this section 2.3, the *Card Design Standards* manual, and the physical, logical, and mobile provisioning security requirements set forth in the following documents, which are found on the PCI SSC website under the **Card Production** filter at https://www.pcisecuritystandards.org/document_library

- *Card Production & Provisioning Physical Security Requirements*
- *Card Production & Provisioning Logical Security Requirements*

Card production activities subject to compliance with these Standards consist of all of the services described in Appendix C of this manual, and which include, by way of example and not limitation, the treatment and safeguarding of Cards, Card manufacture, printing, embossing, encoding, and mailing, as well as to any phase of the production and distribution of Cards or Card account information.

2.3.1 Global Vendor Certification Program

Before employing the services of a vendor to perform any Card production activities, a Customer must ensure that the vendor has been certified by Mastercard under the Global Vendor Certification Program (GVCP).

Prior to certification and annual recertification of a vendor facility under the GVCP, a security assessment of the facility is conducted at approximately 12-month intervals to evaluate the facility's compliance with the PCI documents referenced in section 2.3.

A certified vendor facility is issued a compliance certification, which is subject to annual renewal, provided the vendor facility remains in good standing. The "List of Certified Vendors," as published monthly in a Mastercard Announcement (AN) available on the Technical Resource Center on Mastercard Connect®, contains the name of each vendor facility then certified and a description of the specific services that the facility is authorized to perform.

Any agreement between an Issuer and a vendor for Card production services should contain terms stating that the vendor agrees to safeguard and control usage of Account data and to comply with all applicable Standards then in effect, including but not limited to those set forth in section 2.3 and in the *Card Design Standards* manual.

For more information about the GVCP, contact Mastercard by sending an email message to gvcp-helpdesk@mastercard.com.

2.3.2 Additional Card Production Requirements

Each Issuer must ensure that its Card production activities comply with the following requirements.

Order Request Required to Produce Cards

A vendor must not print or manufacture any Card, sample, or facsimile, on plastic or any other material, except in response to a specific order from a Customer or from Mastercard. To order Cards, a Customer must use the Card Order Request (Form 488), available in the Library section of Mastercard Connect®, or an equivalent document that provides the same information.

Form 488 (or an equivalent document) must be completed and retained by the vendor and Customer, and must be made available to Mastercard upon request.

Mastercard reserves the right to request, from time to time, Card samples for review, and will communicate any such request by way of the **Submit a Card Design Request (Manufacturer)** process on Mastercard Connect®.

Stockpiling Plastics

An Issuer must not encourage a vendor to stockpile plastics or Cards or use a vendor known to engage in the practice of stockpiling plastics or Cards. Stockpiling is the practice of manufacturing excess plastics or Cards in anticipation of future orders from Customers.

Cards Without Personalization

A Customer must not send "unfinished" Cards (as used herein, "unfinished" means a Card that has not yet been personalized with a primary account number [PAN] or expiration date) through the mail. Unfinished Cards must be shipped according to secure shipping methods as described in the *Card Production & Provisioning Physical Security Requirements*. In the rare event that rapid delivery is required and secure shipping methods are infeasible, the Issuer may use an express

courier service that provides shipment tracking, recipient authentication, and receipt confirmation for the shipment of no more than 500 unfinished Cards a day.

Card Count Discrepancies

Upon receiving a shipment of Cards, the Issuer must verify that the correct Card quantity was delivered and take immediate action to resolve any Card count discrepancy and recover any missing Cards. The Issuer may use the Card count noted on each sealed carton in the Card count verification. Sealed cartons may also be opened at random, audited, and resealed. All open cartons and all sealed cartons with no Card count noted on the carton must have the contents counted.

Reporting Card Loss or Theft

Within 24 hours of discovery, a Customer must report to Mastercard the suspected or confirmed loss or theft of any Cards while in transit from a vendor or in the Customer's possession. The report must be sent by email to gvcphelpdesk@ mastercard.com and contain the following information:

- Issuer name and Customer ID/ICA number
- Card type and quantity
- With respect to the loss or theft of Cards while in transit from a vendor:
  - The vendor name
  - The location from which the Cards were shipped
  - The date and method of shipment
  - The address to which the Cards were shipped
- Pertinent details about the loss and the investigation
- Name and phone number of contact for additional information
- Name and phone number of person reporting the loss or theft

Disposition of Unissued Cards and Account Information

A Customer that ceases to issue Cards must promptly destroy or otherwise properly dispose of all unissued Cards and all media containing Account information.

2.4 PIN Security Standards

All Customers and their agents performing PIN encipherment or any other aspect of PIN processing must comply with the applicable PIN security-related requirements in the latest editions of the following documents, available at www.pcisecuritystandards.org:

- *Payment Card Industry (PCI) PIN Security Requirements*
- *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*
- *PCI PTS Hardware Security Module (HSM) Security Requirements*
- *PCI Software-based PIN Entry on COTS (SPoC) Security Requirements*
- *PCI Mobile Payments on COTS (MPoC) Security and Test Requirements*

Cardholder PIN entry at a Terminal must only be performed by means of one of the following:

- A PIN entry device (PED) or an encrypting PIN pad (EPP) evaluated and maintained pursuant to the PCI PTS program; or
- Software-based PIN entry on a COTS device, i.e., PIN entry on the touchscreen of a consumer device (such as a smartphone or tablet). Software-based PIN entry must be driven by a POS Terminal application ("POS App") that is part of either a PCI approved SPoC or MPoC Solution; SPoC and MPoC Solutions, including POS Apps, secure components, and external reading devices/dongles must be evaluated and maintained pursuant to either the PCI SPoC program or the PCI MPoC program, respectively.

As used in this section 2.4, the following terms have the meanings ascribed by the PCI SSC and set forth in the applicable PCI standards documents:

- COTS device
- Attestation and monitoring system
- MPoC Solution
- SPoC Solution

NOTE: All documents referenced in this section 2.4 are available at www.pcisecuritystandards.org.

2.4.1 PIN Entry Devices (PEDs) and Encrypting PIN Pads (EPPs)

PEDs and EPPs are the security hardware and software modules for PIN entry at any type of PIN-capable Terminal, ensuring the confidentiality of the PIN immediately upon entry by the Cardholder. PEDs and EPPs use physical security mechanisms (hardware) as the first line of defense to protect PINs and any other Cardholder data that may be captured by the PED or EPP.

The PCI PTS program for PED and EPP device testing and approval is described in the *Payment Card Industry (PCI) PIN Transaction Security (PTS) Device Testing and Approval Program Guide*. Approved PEDs and EPPs may be found in the *PCI Approved PTS Devices* list at www.pcisecuritystandards.org.

Secure Deployment and Management of PEDs and EPPs

As attackers' security capabilities evolve, the PCI PTS POI specifications for PED and EPP vendors are updated periodically. Acquirers should use the most updated security version of PED and EPP models, as more recent devices offer more robust protections against current threats.

An Acquirer must ensure that all PEDs and EPPs meet the following requirements:

1. Each newly installed PED and EPP must have its model listed in the *PCI Approved PTS Devices* list. Once newly installed, such devices may continue to be used after the expiration of the PCI PTS approval; however, an Acquirer should plan to upgrade or replace the PED or EPP before the expiration of the PCI PTS approval of its model.
2. In limited cases as required by system or business conditions (for example, replacements of faulty devices or refurbishments), an Acquirer may newly install devices from device sets with models whose PCI PTS approval has expired, if either of the following conditions apply:

- The device set is in inventory when the PCI PTS approval expired. Device models that reach approval expiration are moved from the *PCI Approved PTS Devices* list to the *PIN Transaction Security Devices With Expired Approvals* list.
- The device set is under a device management system. Such system must ensure that devices are able to both receive software security patches when made available by the device vendor and are physically managed (for example, maintaining a list of devices and periodically inspecting devices to look for tampering or substitution).

3. An Acquirer must properly manage its PED and EPP inventory. Such management must include:
   - Identifying the type and location of each deployed device; and
   - Having trained staff to conduct periodic visual inspections for signs of tampering or device substitution.
4. In exceptional circumstances, such as widespread successful attacks to a specific model of PED or EPP, Mastercard may, at any point in time, require Acquirers to follow specific risk management actions that may include the sunsetting of that model. Should Mastercard announce a sunset date for a given model, devices of that model, as of the specified sunset date, must no longer be used to process Transactions.

2.4.2 Software-based PIN Entry

Software-based PIN entry occurs on a PIN-enabled COTS device of a merchant using an SPoC or MPoC Solution.

SPoC and MPoC Solutions are composed of several components such as software running on the consumer device, the backend attestation and monitoring system, management services and external reading accessories/dongles. The combination of these components and their security layers ensures the adequate security levels for PIN entry on the touch screen of an MPOS Terminal.

Depending on the configuration offered by vendors, an SPoC or MPoC Solution, its components, or both must be evaluated pursuant to the PCI SPoC program, as described in the *Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC) Program Guide*, or PCI MPoC program, as described in the *PCI Mobile Payments on COTS (MPoC) Program Guide*, respectively.

The lists of SPoC Solutions and associated components validated pursuant to the PCI SPoC program and of MPoC Solutions and associated components validated pursuant to the PCI MPoC program is are available at www.pcisecuritystandards.org.

Secure Deployment and Management of PIN CVM Applications

An Acquirer must ensure that each SPoC Solution or MPoC Solution, and its respective associated components, used by its Merchants and any Sponsored Merchants of a Payment Facilitator of the Acquirer meets the following requirements:

1. The SPoC Solution or MPoC Solution and its associated components is listed by PCI SSC and is in good standing;
2. The POS App is the only Mastercard acceptance application active in the consumer device during the Transaction; and

3. Each Merchant and Sponsored Merchant using the SPoC Solution or MPoC Solution is aware of the associated user guidance.

The attestation and monitoring systems of SPoC Solutions and MPoC Solutions continuously ensures that the overall protection of PIN and Cardholder data is commensurate with current mobile security threat levels.

As attackers' security skills evolve, the attestation and monitoring system of an SPoC Solution or MPoC Solution may determine that a given Solution or an associated component of Such solution is no longer suitable to support secure PIN entry, and may impose Transaction processing restrictions. These restrictions may include halting the full Transaction capability of the Solution.

Variations and Additions by Region

The remainder of this chapter provides modifications to the Standards set out in this chapter. The modifications are organized by region or country and by applicable subject title.

Asia/Pacific Region

The following modifications to the Rules apply in the Asia/Pacific Region or in a particular Region country or countries. Refer to *Mastercard Rules*, Appendix A for the Asia/Pacific Region geographic listing.

2.1 Cybersecurity Standards

In China, the below additional requirements apply:

Cybersecurity Minimum Requirement – China Customers Only

Each Customer must ensure that any Customer environment that stores, processes, or transmits Account Data complies with the security requirements of level 2 or above specified in *Information Security Technology - Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019)* or *Implementation Guideline for Classified Protection of Cybersecurity of Financial Industry (JR/T 0071.2-2020) – Part 2: Basic Requirements*.

Cybersecurity Best Practice – China Customers Only

As a best practice to ensure sufficient cybersecurity controls are established and maintained, all Customer environments, systems, or devices used to store, process, or transmit Account Data and Confidential Information are strongly recommended to comply with at least one of the following:

- *Information Security Technology — Personal information Security Specification (GB/T 35273-2020)*; or
- *Personal Financial Information Protection Technical Specification (JR/T 0171-2020)*

Cybersecurity Validation of Customer – China Customers Only

Prior to the commencement of domestic Transaction processing, each Customer must submit its security compliance validation in accordance with any of the aforementioned security standards. The validation could be the record number and description of the Classified Protection of Cybersecurity or PCI DSS Attestation of Compliance (AOC). Mastercard may require a Customer to provide additional clarification or information of its security practice.

Chapter 3 Card and Access Device Design Standards

This chapter may be of particular interest to Issuers and vendors certified by Mastercard responsible for the design, creation, and control of Cards. It provides specifications for all Mastercard, Maestro, and Cirrus Card Programs worldwide.

3.11 Consumer Device Cardholder Verification Methods

Consumer authentication technologies used on consumer devices, such as personal computers, tablets, mobile phones, and watches, are designed to verify a person as an authorized device user based on one or more of the following:

- "Something I know"—Information selected by and intended to be known only to that person, such as a passcode or pattern
- "Something I am"—A physical feature that can be translated into biometric information for the purpose of uniquely identifying a person, such as a face, fingerprint, or heartbeat
- "Something I have"—Information intended to uniquely identify a particular consumer device

3.11.1 Mastercard Qualification of Consumer Device CVMs

Before a Customer (such as an Issuer or Wallet Token Requestor) may use, as a CDCVM, a consumer authentication technology in connection with the payment functionality of a particular Access Device type (of a specific manufacturer and model), the technology must be submitted to a laboratory approved by EMVCo for a security evaluation, pursuant to the EMVCo Software-Based Mobile Payment (SBMP) approval process. This requirement also applies with respect to any proposed update, change, or modification of the consumer authentication technology that could impact the functionality or security of the CDCVM.

3.11.2 CDCVM Functionality

Mastercard requires testing and certification of each of the following proposed CDCVM functionalities prior to use to effect a Transaction:

1. **Shared Authentication Functionality**—The method used to verify the credentials established by a person in connection with the use of the Access Device or a Digital Wallet on the Access Device also is the method used as the default CDCVM for Transactions involving Accounts accessed by means of the Access Device.
2. **CVM Result Based on Authentication and Explicit Consent**—The Payment Application on the Access Device analyzes the combined result of authentication and consent actions and sets the CDCVM results accordingly. Both Cardholder authentication and explicit Cardholder consent must occur before the Payment Application will complete a Transaction, as follows:
   a. **Cardholder authentication**—The Cardholder may be prompted by the Access Device to perform the CDCVM action at the time of the Transaction, or the CDCVM may consist of a persistent authentication or prolonged authentication in which the CDCVM action is initiated and may also be completed before the Transaction occurs, as described in sections 3.11.3 and 3.11.4.
   b. **Explicit Cardholder consent**—The Cardholder takes a specific Issuer-approved action that serves to confirm that the Cardholder intends a Transaction to be performed. This must consist of an action involving the Access Device that is separate from the act of tapping the Access Device to the Merchant's POS Terminal; for example, the clicking of a button.

3. **Connected Consumer Devices**—If two or more devices in the control of a Cardholder are able to be connected or linked to provide common payment functionality, so that each such device can be an Access Device for the same Account, then Cardholder consent must occur on the Access Device used to effect the Transaction.
4. **Device Integrity**—Upon initiation and continuing throughout Cardholder authentication, the use of the CDCVM must depend on strong device integrity checks. Examples include device runtime integrity checks, remote device attestation, or a combination of both, and checks to ensure that prolonged CVM velocity is intact; for example, the device lock functionality was not disabled.

CDCVM functionality requirements relating to explicit Cardholder consent apply only to the extent that a CVM is requested by the Merchant or Terminal or required by the Issuer for completion of a Transaction. A Cardholder may be offered the option to suppress CDCVM functionality relating to both Cardholder authentication and explicit Cardholder consent solely in connection with Contactless Transactions conducted to obtain transit access (for example, at a turnstile or entry gate). Such Contactless Transactions must be identified with one of the following Card acceptor business codes (MCCs):

- MCC 4111 (Transportation—Suburban and Local Commuter Passenger, including Ferries)
- MCC 4112 (Passenger Railways)
- MCC 4131 (Bus Lines)

In order for a Mobile Payment Device to support CDCVM suppression for transit, its mobile Payment Application must be capable of identifying either of the following conditions in a Contactless Transaction authorization request message:

- A specific bit of Terminal Risk Management Data (Tag 9F1D); or
- One of the above transit MCCs together with a zero Transaction amount.

Either of these conditions enables the Mobile Payment Device to determine that a Contactless Transaction is being conducted for transit access, and not for another purpose (such as the purchase of a monthly transit pass).

3.11.3 Persistent Authentication

Persistent authentication means that authentication of a person as a Cardholder occurs continuously throughout the person's operation of the Access Device, typically through continual contact or biometric monitoring (for example, the monitoring of a heartbeat).

Mastercard requires testing and certification of proposed CDCVM functionality for persistent authentication with respect to the following:

1. A Mastercard-qualified persistence check mechanism is used to detect a change in the person using the device;
2. The device on which authentication is initiated is able to detect without interruption that the authenticated person remains in close proximity to such device or to any connected device with which it shares common payment functionality;

3. The device has the capability to prompt for explicit Cardholder consent (for example, by requiring the Cardholder to click a button or tap on the device) before a Transaction may be effected; and
4. The consumer authentication technology complies with Mastercard Standards.

3.11.4 Prolonged Authentication

Prolonged authentication occurs when a Cardholder authentication (for example, the entry and positive verification of a passcode) remains valid for a period of time (the "open period") and, during that open period, no further authentication is requested or required in order for the Cardholder to effect a Transaction.

Mastercard requires testing and certification of proposed CDCVM functionality for prolonged authentication with respect to the following:

1. The Digital Wallet or Payment Application residing on the device is able to prompt for a new Cardholder authentication based on defined parameter limits;
2. The device is able to prompt for an Issuer-approved form of explicit Cardholder consent (for example, by requiring the Cardholder to click a button or tap on the device) before a Transaction may be effected;
3. The open period of a prolonged Cardholder authentication may be shared by connected or linked consumer devices that are Access Devices for the same Account, provided the Access Devices remain in proximity to one another; and
4. The consumer authentication technology complies with Mastercard Standards.

3.11.5 Maintaining Mastercard-qualified CVM Status

Mastercard may require additional testing of a Mastercard-qualified CDCVM as a condition for the CDCVM to remain a Mastercard-qualified CVM; such requirement may arise, by way of example and not limitation, in the event of any operational, hardware, software, or other technological change that could directly or indirectly impact CDCVM security or other functionality.

Mastercard reserves the right to withdraw Mastercard-qualified CVM status with respect to a CDCVM at any time should Mastercard have reason to believe that the security of the CDCVM is insufficient. Mastercard will notify Customers should a Mastercard-qualified CVM status be withdrawn. Upon publication by Mastercard of such notice, a Customer must immediately cease offering or permitting the use of such consumer authentication technology as a CVM.

3.11.7 Use of a Vendor

Any agreement that a Customer enters into with a vendor for the provision of CDCVM services must include the vendor's express agreement to safeguard and control usage of personal information and to comply with all applicable Standards.

3.12 Card Validation Code (CVC)

3.12.4 Acquirer Requirements for CVC 2

When the Merchant provides the CVC 2 value, the Acquirer must include the CVC 2 value in DE 48, subelement 92 of the Authorization Request/0100 message or Financial Transaction Request/0200 message. The Acquirer is also responsible for ensuring that the Merchant receives the CVC 2 response code provided by the Issuer in DE 48, subelement 87 of the Authorization Request Response/0110 message or Financial Transaction Request Response/0210 message.

An Acquirer must ensure that each of its Merchants that has exceeded 100 gross basis points in fraudulent Card-not-present (CNP) Transactions for two consecutive calendar months:

1. For all MO/TO Transactions, captures and transmits the CVC 2 value to the Issuer for validation; and
2. For all e-commerce Transactions, captures and transmits the CVC 2 value to the Issuer for validation or becomes Mastercard Identity Check™ enabled.

The Acquirer must ensure that the Merchant complies with this requirement within two months following the second trigger month.

In case of BIN attack at a CNP Merchant or Payment Facilitator, the Acquirer, its Service Providers or the affected Merchant or Payment Facilitator must begin to capture and transmit CVC 2 values in all its CNP authorization request messages sent to Issuers within 72 hours (or within a timeframe approved by Mastercard) of the attack detection by the Acquirer, its Service Provider, or the Merchant or notification by Mastercard.

All non-face-to-face gambling Transactions conducted with a Mastercard Card must include the CVC 2 value in DE 48 (Additional Data—Private Use), subelement 92 (CVC 2) of the Authorization Request/0100 message, unless either of the following is present:

- A valid Accountholder Authentication Value (AAV) in DE 48, subelement 43 (Universal Cardholder Authentication Field [UCAF]) resulting from an EMV 3DS authentication; or
- In the case of a recurring payment Transaction, Identity Check Insights (previously known as Data Only).

With the exception of non-face-to-face gambling Transactions, the collection and/or transmission of CVC 2 data is not required when submitting the following types of Card-not-present Transaction authorization requests:

- A valid Accountholder Authentication Value (AAV) resulting from an EMV 3DS authentication or a Digital Secure Remote Payment (DSRP) is present in the authorization request message
- Credential-on-file Transactions (including Account Status Inquiry (ASI) and tokenization requests of a credential-on-file) flagged correctly in the authorization request message
- Identity Check Insights Transactions (previously known as Data Only)
- Transactions involving a Mastercard commercial Card Virtual Account
- Click-To-Pay or Secure Remote Commerce Transactions

3.13 Service Codes

The service code, a three-digit number that complies with ISO/IEC 7813, is encoded on Track 1 and Track 2 of the magnetic stripe of a Card and indicates to a magnetic stripe-reading terminal the Transaction acceptance parameters of the Card. Each digit of the service code represents a distinct element of the Issuer's Transaction acceptance policy. However, not all combinations of valid digits form a valid service code, nor are all service code combinations valid for all Card Programs. Issuers may encode only one service code on Cards, and the same value must be encoded on both Track 1 and Track 2 in their respective, designated positions.

Service codes provide Issuers with flexibility in defining Card acceptance parameters, and provide Acquirers with the ability to interpret Issuers' Card acceptance preferences for all POI conditions.

Service codes apply to magnetic stripe-read Transactions only. In the case of Chip Cards used in Hybrid POS Terminals, the Hybrid POS Terminal uses the data encoded in the chip to complete the Transaction.

NOTE: A value of 2 or 6 in position 1 of the service code indicates that a chip is present on a Card, which contains the Mastercard application that is present on the magnetic stripe.

3.13.2 Acquirer Information

Acquirers must ensure that their Hybrid Terminals do not reject or otherwise decline to complete a Transaction solely because of the service code encoded on the magnetic stripe.

Acquirers are not required to act on the service codes at this time unless:

- A value of 2 or 6 is present in position 1 of the service code for a Mastercard, Maestro, or Cirrus Payment Application. The Hybrid Terminal must first attempt to process the Transaction as a Chip Transaction; or
- The Terminal is located in the Europe Region and has magnetic stripe-reading capability, and a value of 2 is present in position 2 of the service code for a Mastercard Payment Application. The Acquirer must ensure that authorization is obtained before the Merchant completes a magnetic stripe-read Transaction.

3.13.3 Valid Service Codes

Table 3.2 defines service code values for Mastercard, Maestro, and Cirrus Payment Applications and each position of the three-digit service code.

NOTE: Service codes are three positions in length. To identify valid service code values, combine the valid numbers for each of the three positions in this table. The value 000 is not a valid service code and must not be encoded on the magnetic stripe of Mastercard, Maestro, or Cirrus Cards.

Table 3.2—Service Code Values

Definition	Position 1	Position 2	Position 3
International Card	1		
International Card—Integrated Circuit Card	2		
National Use Only	5		
National Use Only—Integrated Circuit Card	6		
Private Label or Proprietary Card	7		
Normal Authorization		0	
Positive Online Authorization Required		2	
PIN Required			0
Normal Cardholder Verification, No Restrictions			1
Normal Cardholder Verification—Goods and services only at Point of Sale (no cash back)			2
ATM Only, PIN Required			3
PIN Required—Goods and services only at Point of Sale (no cash back)			5
Prompt for PIN if PIN Pad Present			6
Prompt for PIN if PIN Pad Present—Goods and services only at Point of Sale (no cash back)			7

3.13.4 Additional Service Code Information

The following information explains the service code values in Table 3.2.

- Normal authorization is an authorized Transaction according to the established rules governing Transactions at the POI.
- Positive Online Authorization Required service codes (value of 2 in position 2) indicate that an electronic authorization must be requested for all Transactions. This service code value is optional for Mastercard Unembossed Cards.

- Normal Cardholder verification indicates that the CVM must be performed in accordance with established rules governing Cardholder verification at the POI.
- ICC-related service codes (value of 2 or 6 in position 1) are permitted only on Chip Cards containing a Mastercard, Maestro, or Cirrus Payment Application type-approved by Mastercard or its agent.
- ICC-related service codes (value of 2 or 6 in position 1) may not be used for stand-alone stored value (purse) applications that reside on Mastercard, Maestro, or Cirrus Cards. In these instances, a value of 1 must be placed in the first position.
- National Use Only service codes (value of 5 or 6 in position 1) are permitted only on National Use Only Cards approved by Mastercard. This includes PIN-related service codes on **National Use Only** Cards (for example, 506) governed by local PIN processing rules.
- Private label or proprietary service codes (value of 7 in position 1) on Cards that contain a valid Mastercard BIN are permitted only on private label or proprietary Cards approved by Mastercard.

Issuers may not use PIN-related service codes for Card Programs unless Mastercard has approved the indicated use of a PIN.

Chapter 4 Terminal, PIN, and MFA Method Security Standards

This chapter may be of particular interest to Customers that support or enable PIN as a Cardholder Verification Method (CVM) or Multi-Factor Authentication (MFA) Methods for Remote Commerce Token Transactions. Refer to the applicable technical specifications and the Transaction Processing Rules manual for additional Terminal and Transaction processing requirements relating to the use of a PIN.

4.1 Personal Identification Numbers (PINs)

The personal identification number (PIN) allows Cardholders to access the Mastercard® ATM Network accepting the Mastercard®, Maestro®, and Cirrus® brands, and to conduct Transactions at Cardholder-activated Terminal (CAT) 1 devices, Maestro Merchant locations, and Hybrid Point-of-Sale (POS) Terminals.

PIN security requirements and best practices for Acquirers are described in this chapter and in section 2.4. PIN security best practices for Issuers are described in the *Issuer PIN Security Guidelines*.

4.5 PIN Encipherment

All Customers and their agents performing PIN Transaction processing must comply with the security requirements for PIN encipherment specified in the *Payment Card Industry PIN Security Requirements*.

An Acquirer must ensure that PIN entry devices (PEDs) and encrypting PIN pads (EPPs) comply with the following requirements:

- For secure transmission of the PIN from the PED or EPP to the Issuer host system, the PED or EPP must encrypt the PIN using the approved algorithm(s) for PIN encipherment listed in ISO/IEC 9564-2 (Financial services—PIN management and security—Part 2: Approved algorithms for PIN encipherment) and the appropriate PIN block format as provided in ISO/IEC 9564-1 (Financial services—PIN management and security—Part 1: Basic principles and requirements for PINs in card-based systems); and
- If the PIN pad and the secure component of the PED are not integrated into a single tamper-evident device, then for secure transmission of the PIN from the PIN pad to the secure component, the PIN pad must encrypt the PIN using the approved algorithm(s) for PIN encipherment listed in ISO/IEC 9564-2.

All Issuers and their agents performing PIN processing should also refer to the Mastercard *Issuer PIN Security Guidelines* document regarding PIN encipherment.

Refer to *China Switch Specifications* for PIN encipherment requirements applicable to China domestic Transactions.

4.6 PIN Key Management

Key management is the process of creating, distributing, maintaining, storing, and destroying cryptographic keys, including the associated policies and procedures used by processing entities.

All Acquirers and their agents performing PIN Transaction processing must comply with the security requirements for PIN and key management specified in the *Payment Card Industry PIN Security Requirements*.

In addition, all Acquirers and their agents must adhere to the following Standards for PIN encryption:

1. Perform all PIN encryption, translation, and decryption for the network using hardware encryption.
2. Do not perform PIN encryption, translation, or decryption using software routines.

All Issuers and their agents performing PIN processing should refer to the *Issuer PIN Security Guidelines* regarding all aspects of Issuer PIN and PIN key management, including PIN selection, transmission, storage, usage guidance, and PIN change.

4.6.1 PIN Transmission Between Customer Host Systems and the Interchange System

The Interchange System and Customers exchange PIN encryption keys (PEKs) in two manners: **statically** and **dynamically**. Directly connected Customers that are processing Transactions that contain a PIN may use either static or dynamic key encryption to encipher the PIN.

Mastercard strongly recommends using dynamic PEKs. Static PEKs must be replaced as indicated in the references below.

For information about PIN key management and related services, including requirements for key change intervals and emergency keys, refer to the manuals listed in Table 4.1, which are available through the Mastercard Connect® Publications product.

Table 4.1—PIN Key Management References

For Transaction authorization request messages routed through...	Refer to...
Mastercard Network/Dual Message System	*Authorization Manual*
Mastercard Network/Single Message System	*Single Message System Specifications*
Mastercard Key Management Center through the On-behalf Key Management (OBKM) Interface	*On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications*

4.6.2 On-behalf Key Management

Mastercard offers the On-behalf Key Management (OBKM) service to Europe Region Customers as a means to ensure the secure transfer of Customer cryptographic keys to the Mastercard Key Management Center. OBKM services offer Customers three key exchange options:

- **One-Level Key Hierarchy**—Customers deliver their cryptographic keys in three clear text components to three Mastercard Europe security officers. The security officers then load the key components into the Key Management Center.
- **Two-Level Key Hierarchy**—The Key Management Center generates and delivers transport keys to Customers in three separate clear text components. Customers use the transport keys to protect and send their cryptographic keys to Key Management Services in Waterloo, Belgium. Key Management Services then loads the Customer keys into the Key Management Center.
- **Three-Level Key Hierarchy**—The Key Management Center uses public key techniques to deliver transport keys to Customers in three separate clear text components. Customers use the transport keys to protect and send their cryptographic keys to Key Management Services in Waterloo, Belgium. Key Management Services then loads the Customer keys into the Key Management Center.

Mastercard recommends that Customers use the Two-Level or Three-Level Key Hierarchy, both of which use transport keys to establish a secure channel between the Customer and the Key Management Center.

Mastercard has developed a Cryptography Self Test Tool (CSTT) to assist Customers in meeting OBKM interface requirements. Customers must use the CSTT before exchanging keys with Key Management Services using the Two-Level and Three-Level Hierarchies.

Customers must register to participate in the OBKM service. For more information, contact key_management@mastercard.com or refer to the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications*, available through the Mastercard Connect® Publications product.

4.7 Terminal Security Standards

The Acquirer must ensure that each Terminal:

1. Has a magnetic stripe reader capable of reading Track 2 data and transmitting such data to the Issuer for authorization;
2. Permits the Cardholder to enter PIN data in a private manner;
3. Prevents a new Transaction from being initiated before the prior Transaction is completed; and
4. Validates the authenticity of the Card or Access Device.

For magnetic stripe Transactions, the following checks must be performed by the Acquirer (either in the Terminal or the Acquirer host system), before the authorization request is forwarded:

1. **Longitudinal Redundancy Check (LRC)**—The magnetic stripe must be read without LRC error.
2. **Track Layout**—The track layout must conform to the specifications in Appendix A.

With respect to the electronic functions performed by a Terminal, the following requirements apply:

1. A Transaction may not be declined due to bank identification number (BIN)/Issuer identification number (IIN) validation.
2. A Transaction may not be declined as a result of edits or validations performed on the primary account number (PAN) length, expiration date, service code, discretionary data, or check digit data of the Access Device.
3. Tests or edits on Track 1 must not be performed for the purpose of disqualifying a Card from eligibility for Interchange System processing.

Refer to section 2.4 for PIN-related security requirements.

4.8 Hybrid Terminal Security Standards

The Acquirer must ensure that a Hybrid Terminal deployed at a location where any Mastercard brands are accepted complies with all of the following Standards:

- Each Hybrid Terminal that reads and processes EMV-compliant payment applications must read and process EMV-compliant Mastercard-branded Payment Applications.
- Each Dual Interface Hybrid Terminal must read and process the same Mastercard-branded Payment Applications on both the contact and contactless interfaces.
- Each Hybrid Terminal must perform a Chip Transaction when a Chip Card or Access Device is presented in compliance with all applicable Standards, including those Standards set forth in the *M/Chip Requirements for Contact and Contactless* manual.
- A Terminal deployed in China must additionally comply with PBoC's latest chip standard and utilize the SM cryptography to perform China domestic Transactions in accordance with China regulatory requirements. Refer to the *China Market Terminal Requirements* for more information.

4.9 Triple DES Standards

Triple Data Encryption Standard (DES), minimum double key length (hereafter referred to as Triple DES), must be implemented as follows:

- All newly installed PEDs, including replacement and refurbished PEDs that are part of POS Terminals, must be Triple DES capable. This requirement applies to POS Terminals owned by Customers and non-Customers.
- All Customer and processor host systems must support Triple DES.
- It is strongly recommended that all PEDs that are part of POS Terminals be Triple DES compliant and chip-capable.
- All EPPs that are part of ATM Terminals must be Triple DES compliant.
- All Transactions routed to the Interchange System must be Triple DES compliant.

Mastercard recognizes that Customers may elect to use other public key encryption methods between their POS Terminals or ATMs and their host(s). In such instances, Mastercard must approve the alternate method chosen in advance of its implementation and use.

Approval will be dependent, in part, on whether Mastercard deems the alternate method to be as secure as or more secure than Triple DES. **Approval is required before implementation can begin**.

4.10 Multi-Factor Authentication Methods for Remote Commerce Token Transactions

Subject to any regulatory approvals and compliance with applicable laws and regulation, Cardholder authentication technologies may be implemented by an entity (herein, the "Authenticating Entity") in remote commerce use cases, to verify a person as an authorized Cardholder based on the use of two or more authentication factors. Each factor must belong to one of the three following categories, with no more than one authentication factor coming from any one category.

- Possession factor, defined as "something only the user possesses" such as personal computers, tablets, mobile phones, IoT devices (such as connected cars) and security tokens.
- Knowledge factor, defined as "something only the user knows" such as PINs or passwords, which are either:
  - Fully managed by the Authenticating Entity, such as a password or PIN created and verified by the Authenticating Entity.
  - Shared with the operating system on the Cardholder's consumer device, such as a password or PIN defined by the Cardholder for consumer device access and which can be used across multiple applications; it is created and verified locally by the consumer device's operating system (for example, Android, iOS, MAC OS, Windows)
- Inherence factor, defined as "something the user is"; it includes several categories of factors that can be used for the purpose of uniquely identifying a person:
  - Physical biometrics like fingerprint, physiological or facial recognition.
  - Behavioral biometrics that relate to behavioral processes created for example by the human body, the way that Cardholders tap on, type, swipe or hold a device.
  - Where allowed under applicable legislation, behavioral-based inherence information generated from multiple data points that include elements identifying, for example, the Cardholder's location, spending habits and Transaction history.

4.10.1 Security Evaluation of Multi-Factor Authentication Methods

Before an Authenticating Entity may use an MFA Method to verify a person as an authorized Cardholder, the MFA Method must be Mastercard-qualified per the process defined in the below paragraph.

The consumer authentication technology in connection with the payment application that analyzes the results of the authentication must be submitted to a laboratory accredited by Mastercard for a security evaluation, pursuant to the Mastercard Compliance Assessment and Security Testing (CAST) process.

This requirement also applies with respect to any proposed update, change, or modification of the consumer authentication technology that could impact the functionality or security of the MFA Method. Following successful completion of the security evaluation, the Method will be qualified as a high assurance Method.

Pending Mastercard approval, the MFA Method may go through a security evaluation performed outside of a laboratory accredited by Mastercard, and be qualified as a low assurance Method instead. In this case, the entity certifying the Method must be an independent auditor that performs other certifications or similar activity.

In the EEA, San Marino, United Kingdom, and Gibraltar, MFA Methods are subject to the audit requirements set out in Article 3 of the PSD2 RTS on SCA and UK Technical Standards on SCA.

The level of assurance may be a relevant factor in Issuer reliance on the solution for fraud deterrence.

4.10.2 Multi-Factor Authentication Method Functionality

Mastercard requires testing and certification of each of the following Multi-Factor Authentication Method functionalities prior to use to effect a Transaction:

1. **Accuracy of the Method**
   a. **False Matches:** The Method must generate a False Match Rate of no greater than 0.01%.
   b. **False Non-Matches:** The Method should generate a False Non-Match Rate of no greater than 3%.
   c. Additional performance requirements may apply for inherence factors.

   When the Authenticating Entity depends on an operating system's capabilities to handle Cardholder authentication such as fingerprint, facial recognition, PIN, password, or pattern, the platforms on which the MFA solution is permitted to function must meet the above requirements.
2. **Security of Authentication Factors**
   The Method must use Authentication factors subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the Factors does not compromise the reliability of the other Factors.
3. **Binding of the Method to the authorized Cardholder**
   The Authenticating Entity must use an approved Identification & Verification (ID&V) method to validate that the End User is the authorized Cardholder and must subsequently bind, within five minutes of the ID&V, the token to a reference to the MFA Method. When the MFA Method includes a consumer device as possession factor, the Authenticating Entity must bind the Token to a reference to the consumer device. The Token is then considered to be a device-bound Token.

   In the EEA, San Marino, United Kingdom, and Gibraltar, the Issuer must ensure that the ID&V method complies with the Strong Customer Authentication (SCA) requirements set out in the applicable legislation on SCA.
4. **Authentication Result Based on Authentication and Explicit Consent**

The Authenticating Entity's server analyzes the combined result of authentication and consent actions and sets the Authentication results accordingly. Both Cardholder authentication and explicit Cardholder consent must occur prior to use to effect a Transaction, as follows:

a. **Cardholder authentication:** The Cardholder may be prompted to authenticate with the MFA Method at the time of the Transaction, or the authentication may consist of a persistent authentication or prolonged authentication in which the authentication is initiated with the MFA Method at a time before the Transaction occurs, as described in sections 4.10.3 and 4.10.4.
b. **Explicit Cardholder consent:** The Cardholder takes a specific action that serves to confirm that the Cardholder intends a Transaction to be performed. This must consist of an action involving the Cardholder for example, by clicking a button on the Authenticating Entity interface, or providing voice instructions.

5. **Device integrity**
The Authenticating Entity must ensure that they adopt security measures to mitigate the risk which results from the device being compromised. The mitigating measures shall include each of the following:

a. The use of separated secure execution environments through the software installed inside the device.
b. Mechanisms to ensure that the software or device has not been altered by the Cardholder or by a third party – and, where alterations have taken place, mechanisms to mitigate the consequences thereof.

6. **Failed Authentication**
The Authenticating Entity must ensure that the Multi-Factor Authentication Method includes each of the following measures:

a. The number of failed authentication attempts that can take place consecutively shall not exceed five within a given period determined by the Authenticating Entity, after which further attempts at Authentication shall be temporarily or permanently blocked. The duration of the block shall be established in accordance with the relevant risks involved.
b. The block will become permanent if there are too many unsuccessful authentication attempts or if there is a chance of compromise. Before the block is made permanent, the Cardholder should be notified.
c. When the block has been made permanent, a new ID&V must be established allowing the consumer to regain use of the blocked payment card. Authenticating Entities must not use alternate methods to recover the use of an authentication factor; for example, a link sent by email to reset a password and define a new one.

4.10.3 Persistent Authentication

Persistent Authentication means that the authentication performed by the Authenticating Entity on a Cardholder's personal Internet-of-Things (IoT) device (such as a connected car) occurs continuously throughout the Cardholder's operation of that personal IoT device, through

continual contact or biometric monitoring (for example, the monitoring of the Cardholder's presence in a connected car).

A successful Persistent Authentication will be dependent upon an initial authentication performed by the Authenticating Entity with the MFA Method when the Cardholder initiates or operates the IoT personal device, for example, when a Cardholder engages with a connected car.

For Persistent Authentication, the Authenticating Entity must ensure that it has:

- Approval from Mastercard to implement Persistent Authentication for an IoT device use case; and
- Any necessary regulatory approvals needed for the Persistent Authentication and that the use of the Persistent Authentication complies with all applicable regulations.

For the Authenticating Entity to perform Transactions without the use of the MFA Method to authenticate the Cardholder, Mastercard requires testing and certification of proposed functionality for Persistent Authentication with respect to the following:

- There is an inherence factor integrated within the IoT personal device, or there is a persistent check mechanism incorporated in the IoT personal device, used to detect a change in the status of the Cardholder using the device, through a combination of on-body detection mechanisms and other signals (for example, the monitoring of the Cardholder's presence in a connected car signals that it is the same car, and the doors are closed). The check/locking mechanism must be sufficiently secure to ensure that only the person who performed the initial strong customer authentication continues to be the person in possession of and operating the IoT personal device.
- The IoT device on which the MFA Method has been applied must be disabled for authentication purposes within a maximum of three seconds of the Cardholder detection.
- The Cardholder provides an explicit consent to the transaction, for example, by clicking a button on the Authenticating Entity interface, on which the transaction amount and merchant identification are both displayed or by providing voice instructions.
- The length of duration for Persistent Authentication may not exceed twentyfour hours.
- When the period ends, a new period can start after a successful authentication performed by the Authenticating Entity with the MFA Method.

4.10.4 Prolonged Authentication

Prolonged Authentication occurs when a Cardholder authentication (for example, the positive verification of fingerprint authentication on a consumer device) remains valid for a period of time (the "open period") and, during that open period, the completion of an MFA Method is not requested or required in order for the Cardholder to effect a Transaction.

The Authenticating Entity must ensure that it has any necessary regulatory approvals needed for the Prolonged Authentication and that the use of the Prolonged Authentication complies with all applicable regulations.

A successful Prolonged Authentication will be dependent upon an initial authentication performed by the Authenticating Entity with the MFA Method; for example, an authentication performed before a Cardholder can access a Stored Credential.

For the Authenticating Entity to perform a transaction without the use of the MFA Method, Mastercard requires testing of the proposed functionality for Prolonged Authentication with respect to the following:

- The Cardholder provides an explicit consent before a Transaction may be effected, for example, by clicking a button on the Authenticating Entity interface.
- The Authenticating Entity authenticates the Cardholder with one Authentication factor, which may be an existing factor of the MFA Method (in the EEA and United Kingdom, this is in order to comply with the dynamic linking requirement); and
- The open period ends, which may not exceed five continuous minutes

4.10.5 Maintaining Mastercard-qualified Multi-Factor Authentication Method

Mastercard may require additional testing of a Mastercard-qualified MFA Method as a condition for the Method to remain a Mastercard-qualified Method; such requirement may arise, by way of example and not limitation, in the event of any operational, hardware, software, or other technological change that could directly or indirectly impact the Method security or other functionality.

Mastercard reserves the right to withdraw Mastercard-qualified status with respect to an MFA Method at any time should Mastercard have reason to believe that the security of the Method is insufficient. Mastercard will notify Authenticating Entities should a Mastercard-qualified status be withdrawn. Upon publication by Mastercard of such notice, an Authenticating Entity must immediately cease offering or permitting the use of such consumer authentication technology as an MFA Method.

4.10.6 Use of a Vendor

Any agreement that an Authenticating Entity enters with a vendor for the provision of Multi-Factor Authentication Method services must include the vendor's express agreement to safeguard and control usage of personal information and to comply with all applicable Standards.

Chapter 5 Card Recovery and Return Standards

This chapter may be of particular interest to Customers that issue Mastercard® Cards. It includes guidelines for personnel responsible for Card retention and return, reporting of lost and stolen Cards, and criminal and counterfeit investigations.

5.1 Card Recovery and Return

The following sections address Customer responsibilities associated with Card retention and return, rewards for Card capture, reporting of lost and stolen Cards, and criminal and counterfeit investigations.

5.1.1 Card Retention by Merchants

Acquirers and Merchants should use their best efforts to recover a Card by reasonable and peaceful means if:

- The Issuer advises the Acquirer or Merchant to recover the Card in response to an authorization request.
- The Electronic Warning Bulletin file or an effective regional *Warning Notice* lists the account number.

After recovering a Card, the recovering Acquirer or Merchant must notify its authorization center or its Acquirer and receive instructions for returning the Card. If mailing the Card, the recovering Acquirer or Merchant first should cut the Card in half through the magnetic stripe.

Maestro Card capture at a Point-of-Sale (POS) Terminal is not permitted with respect to Interregional Transactions or Intraregional Transactions that occur within the Asia/Pacific, Latin America and the Caribbean, or United States Regions.

5.1.1.1 Returning Recovered Cards

The Acquirer must follow these procedures when returning a recovered Card to the Issuer:

1. If the Merchant has not already done so, the Acquirer must render the Card unusable by cutting it in half vertically through the magnetic stripe.
2. The Acquirer must forward the recovered Card to the Issuer within five calendar days of receiving the Card along with the first copy (white) of the Interchange Card Recovery Form (ICA-6). The additional copies are file copies for the Acquirer's records. Unless otherwise noted in the "Other Information" section of the Company Contact Management application, a recovered Card must be returned to the Security Contact of the Issuer.

NOTE: A sample of the Interchange Card Recovery Form (ICA-6) appears in the Forms section of Mastercard Connect®.

A Merchant may return a Card inadvertently left at the Merchant location if the Cardholder claims the Card before the end of the next business day and presents positive identification. With respect to unclaimed Cards, a Merchant must follow the Acquirer's requirements as set forth in the Merchant Agreement.

5.1.1.2 Returning Counterfeit Cards

The Acquirer or Merchant must return counterfeit Cards to the Issuer by following the instructions provided by its authorization center. The following information identifies an Issuer:

- The Issuer's name and/or logo on the Card front
- The Licensee Acknowledgement Statement

In the absence of an Issuer's name/logo or Licensee Acknowledgement Statement, the Issuer may be identified by any other means, including the Issuer's Mastercard bank identification number (BIN) printed on the front or back of the Card or the magnetic stripe. If the Issuer is still unidentifiable, return the Card to the Franchise Department at the address provided in Appendix B.

NOTE: The above method of identifying the Issuer applies only to the return of a counterfeit Card, not to determining the Customer responsible for the counterfeit losses associated with such Cards. For more information, refer to Chapter 6—Fraud Loss Control Standards of this manual.

5.1.1.3 Liability for Loss, Costs, and Damages

Neither Mastercard nor any Customer shall be liable for loss, costs, or other damages for claims declared against them by an Issuer for requested actions in the listing of an account or a Group or Series listing on the Electronic Warning Bulletin file or in the applicable regional *Warning Notice* by the Issuer. Refer to the *Account Management System User Manual* for information about the procedures for listing accounts.

If an Acquirer erroneously uses these procedures without the Issuer's guidance and authorizes Merchant recovery of a Card not listed on the Electronic Warning Bulletin file or in the applicable regional *Warning Notice*, neither Mastercard or its Customers shall be liable for loss, costs, or other damages if a claim is made against them.

No Customer is liable under this section for any claim unless the Customer has:

- Written notice of the assertion of a claim within 120 days of the assertion of the claim, and
- Adequate opportunity to control the defense or settlement of any litigation concerning the claim.

5.1.2 ATM Card Retention

Card retention must occur only at the Issuer's command. Cards captured because of ATM Terminal malfunction or Cardholder error, over which the ATM Terminal owner has no control, are the only allowable exceptions. If the ATM Acquirer cannot determine within two business days if a Card was captured because of a machine malfunction, Cardholder error, or a command sent by the Issuer, the Card will be deemed to be a Card captured on command of the Issuer.

An ATM Terminal Acquirer that as an Issuer sends Card capture commands must honor the commands sent by other Issuers at all of its ATMs that are capable of Card capture.

In the Europe Region, the Acquirer of any ATM Terminal capable of Card capture must honor the Card capture commands sent by any Issuer.

Completion messages must indicate, to the best knowledge of the Acquirer, the action taken by the ATM for each Card capture request.

5.1.2.1 Handling ATM-Retained Cards

An ATM Terminal Acquirer must handle retained Cards in accordance with the following requirements:

1. Log all retained Mastercard® Cards under dual control immediately upon removal from the ATM. With respect to retained Maestro® and Cirrus® Cards, it is the responsibility of the Acquirer to establish appropriate procedures for documenting a Card capture.
2. Destroy retained Cards by cutting them in half vertically through the magnetic stripe, if the Card is captured on command of the Issuer or if an Acquirer's procedures do not include returning retained Cards to Cardholders. A Maestro Card issued outside of the Europe Region and captured by an ATM Terminal located in the Europe Region must be destroyed and discarded.

When a captured card appears to be fraudulent (for example, a plain white plastic or cardboard card), the Acquirer may (at its option) retain, preserve, and release such card to appropriate law enforcement authorities.

5.1.2.2 Returning ATM-Retained Cards to Cardholders

Cards retained at the request of an Issuer must never be returned to the Cardholder without the permission of the Issuer. However, Cards erroneously retained by the Acquirer because of a machine malfunction, system failure, or Cardholder error may be held at the ATM location, in a secure place, for two business days following capture and released to the Cardholder subsequent to all of the following:

1. The Acquirer checks the Electronic Warning Bulletin file or applicable regional *Warning Notice* (required for Mastercard Cards only).
2. The Cardholder presents reasonable identification (for example, a current driver's license, passport, or similar identification with a picture or descriptive data and a signature that is comparable to the signature on the captured Card, if applicable).
3. The Cardholder signs a disposition log or receipt, or the Acquirer otherwise maintains a record of the action taken.

The Acquirer then must notify the Issuer and explain that the Card was retained, the circumstances of the retention, and that the Card was returned to the Cardholder.

If the Cardholder does not return to claim the Card before the end of the second business day following Card capture, the Card's magnetic stripe must be destroyed.

An Acquirer will not incur liability for fraudulent or unauthorized Transactions initiated with a Card that such Acquirer has returned to a Cardholder following the Card's capture at an ATM Terminal, provided that the Acquirer complied with the requirements described in this section.

5.1.2.3 Fees for ATM Card Retention and Return

The Acquirer must not charge the Issuer any fee for the ATM retention or return of a Card.

5.1.3 Payment of Rewards

The Acquirer may, at its option, pay the Merchant or financial institution teller a reward for capturing a Card in accordance with local practice. The person capturing the Card receives the reward.

5.1.3.1 Reward Payment Standards

The Acquirer must follow these Standards when paying a reward:

1. Pay no less than USD 50 to the Merchant capturing a Card listed on the Electronic Warning Bulletin file or in the *Warning Notice* and no less than EUR 50 to the Merchant capturing a Card listed under Region D on the Electronic Warning Bulletin file.
2. Pay the Merchant USD 100 (EUR 100 when the Merchant is in the Europe Region and the valid Card was issued in the Europe Region), **if** a Merchant initiates an authorization call because of a suspicious Transaction or captures a Card not listed on the Electronic Warning Bulletin file or in the *Warning Notice*.
3. Pay a reward to a financial institution teller for the capture of another Customer's Card if it is the Acquirer's practice to pay its tellers rewards for picking up its own Cards. The amount of the reward should be the same amount paid for the capture of the Acquirer's own Cards within the limits set forth in section 5.1.3.2.
4. Charge the Issuer for reimbursement of the reward paid upon dispatching each Card captured by either a Merchant or a financial institution teller. The Fee Collection/1740 message with an Integrated Product Messages (IPM) message reason code (Data Element 25) equal to 7601 will settle the reward.

5.1.3.2 Reward Amounts

The Acquirer should follow these guidelines for determining reward amounts.

Table 5.1—Amount Determinations

IF the capture...	THEN pay this amount...
Resulted from a "Merchant Suspicious" phone call	USD 100 (EUR 100 when the Merchant is in the Europe Region and the valid Card was issued in the Europe Region)
Did not result from a "Merchant Suspicious" phone call	USD 50 (EUR 50 in the Europe Region)
Leads to the capture of additional Cards	USD 50/EUR 50 for each Card captured, with a maximum total of USD 250/EUR 250 for any one incident

The stipulation that the person capturing the recovered Card receives the reward as stated in section 5.1.3 does not prevent Customers from making mutually acceptable agreements between themselves regarding rewards.

The recovering Customer may collect an administrative fee of USD 15 for expenses incurred in processing the captured Card. A recovering Customer in the Europe Region may collect an administrative fee of EUR 15 for such expenses. The capturing Customer may add this fee to the amount of the reward reimbursement or collect the fee independently, using the Fee Collection/1740 message.

5.1.3.3 Reimbursement of Rewards

The following specifications apply to reward reimbursement:

- Upon dispatching the Card to the Issuer, the Acquirer will obtain reimbursement for the reward paid and the USD 15 or EUR 15 fee by processing the Fee Collection/1740 message.
- If a Customer returns a Card to an Issuer and a reward is not paid, the recovering Customer may, at its discretion, collect a USD 15 or EUR 15 fee by processing a Fee Collection/1740 message record.
- Upon receipt of the Interchange Card Recovery Form (ICA-6), the Issuer should match it to the Fee Collection/1740 message record based on the Acquirer Member ID, account number, and recovery date comparisons.

5.1.3.4 Reward Payment Chargebacks

A reward reimbursement draft may be charged back only when the incorrect Customer is charged. The senior vice president of the Franchise Department will resolve any dispute concerning reward reimbursement.

Chapter 6 Fraud Loss Control Standards

This chapter may be of particular interest to personnel responsible for fraud loss control programs, counterfeit loss procedures and reimbursement, and Acquirer counterfeit liability.

6.2 Mastercard Fraud Loss Control Program Standards

The existence and use of meaningful controls are an effective means to limit total fraud losses and losses for all fraud types. This section describes minimum requirements for Issuer and Acquirer fraud loss control programs.

6.2.2 Acquirer Fraud Loss Control Programs

An Acquirer must establish, and ensure that each of its Service Providers, ATM owners, and other agents implement, a fraud loss control program that meets the following minimum requirements, and preferably will include the recommended additional parameters.

The program must automatically generate daily fraud monitoring reports and realtime or near-real-time alerts.

An Acquirer must have the capability to stop the authorization flow related to fraudulent Transactions, in case of major fraud attack, emergency situations or at Mastercard's request.

The Acquirer or its Service Provider must have staff trained to write fraud detection rules and manage fraud cases.

Alerts and Daily fraud monitoring reports must be analyzed by trained staff within 24 hours and measures be implemented to mitigate fraud as soon as possible and at the latest within 72 hours following the Transactions time.

6.2.2.1 Acquirer Authentication Strategy

Requirements

An Acquirer and its Service Providers must comply with the relevant authentication requirements set forth in the Standards, including but not limited to:

- *Mastercard Identity Check™ Program Guide*
- *Mastercard Identity Check™ Compliance Program Guide*
- *Authentication Guide for Europe* (applicable to Europe Region Acquirers only)

An Acquirer must implement strong authentication controls (ideally two factors) to ensure that only the Acquirer, its Service Providers (for example, any 3-D Secure Service Provider operating a 3-D Secure server, Third Party Processor, or Payment Facilitator) and its Merchants can initiate Transactions on its platform.

Effective 13 October 2023, an Acquirer in the Europe Region, excluding Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Serbia, Tajikistan, Turkey, Turkmenistan, Ukraine, and Uzbekistan, must comply with the following additional requirement:

At the time of storing a Credential on file or in a wallet or Tokenizing a Credential, or at the latest during the first Transaction following Card-add, the Acquirer must ensure that the Acceptor either successfully completes an EMV 3DS authentication (i.e., challenge IND = 04/SCA mandated, and RREQ = Y) or applies another method that results in completed SCA with Issuer step-up.

Recommendations

An Acquirer is recommended to implement the following with each of its Merchants and Payment Facilitators:

- The authentication recommendations listed in *Mastercard Identity Check™ Program Guide*
- Implement MDES for Merchant (M4M) to replace real card data by tokenized and digitized payment credentials (tokens)
- EMV Chip Terminals with PIN Capability (Please refer to existing mandates in specific countries)

The MCC submitted at the time of authentication should match the MCC submitted at the time of the authorization except when a single authentication relates to multiple authorizations for different merchants.

Addressing BIN Attacks

BIN attacks either detected by the Acquirer or communicated to the Acquirer by Mastercard, must be mitigated by the Acquirer, its processor(s) or the concerned Merchant(s) within 72 hours (or within a timeframe approved by Mastercard) of detection by the Acquirer, its Service Provider, the Merchant or notification by Mastercard.

By way of example, an attack will be qualified as a BIN attack when the following two conditions are met:

1. At least 100 authorization requests or authentication requests are sent within one hour for the BIN or BIN Account range from one or more Merchants.
2. The Issuer, its Service Provider, or Mastercard (using a network fraud detection tool) declined fifty percent (50%) or more of the authorization requests or authentication requests within one hour.

An Acquirer must also analyze each BIN or BIN Account range attack to identify its modus operandi and implement corrective measures to prevent future attacks using the same technique(s).

Suspicious ATM Activity

Each ATM Terminal Acquirer and its Service Providers or other agents acting on its behalf must have sufficient controls, resources and monitoring systems for the prompt detection and reporting of suspicious ATM activity as required by Mastercard Rule 1.2.

ATM Terminal Acquirers are obligated under Mastercard Rule 1.2 to monitor and report suspicious ATM Transaction activity, regardless if the issuer has or has not reported the activity as fraud. Suspicious money laundering activity may include, but is not limited to:

- Out-of-pattern ATM withdrawal volume and/or velocity at an individual ATM or groups of ATMs
- Sequential or consecutive high volumes of ATM withdrawals at the same ATM(s) by multiple cards from the same issuer
- Significantly high volumes of repetitive ATM withdrawal amount consistently over time

- Excessive ATM withdrawals at maximum Transaction limits of ATM in a short period of time
- Out-of-pattern excessive or high volumes of ATM deposits

ATM Authorization Controls and Cash-out Attack Management

Each ATM Terminal Acquirer and its Service Providers must, upon detecting a cash-out attack or receiving notification from Mastercard or a Mastercard solution (for example, Safety Net Alert) of a confirmed cash-out attack:

- Block acceptance of the BIN under attack at the ATM Terminal within five hours (unless Mastercard notifies the Acquirer that Mastercard has taken action to stop the attack)
- If requested by Mastercard, following issuer confirmation of an attack, acquirer is recommended to contact law enforcement for initiating an investigation of the on-going attack, including if possible, the detection and communication of ATM address in real-time (or quasi-real time) to Law Enforcement.
- If the ATMs are equipped with a camera, acquirers are recommended to safeguard the video recording for sharing with Law Enforcement where legally allowed.

An Acquirer of ATM Transactions must ensure that each Service Provider acting on its behalf has the capability, upon detection of suspected fraud, to adjust (typically reduce) the maximum withdrawal amount per Transaction at individual ATM Terminals to mitigate potential losses.

6.2.2.2.1 Additional Acquirer Authorization Monitoring Requirements for Negative Option Billing Merchants

In addition to the Acquirer authorization monitoring requirements listed in section 6.2.2.2 of this manual, an Acquirer of a negative option billing Merchant must monitor authorization Transaction messages to identify when the same Account number appears among different negative option billing Merchant IDs in the Acquirer's Portfolio within 60 calendar days.

When the Acquirer identifies such an Account, the Acquirer must take reasonable steps to verify that each Transaction conducted by the valid Cardholder with the associated negative option billing Merchant is a bona fide Transaction. This verification may include, but is not limited to, an electronic copy or hard copy of the Transaction information document (TID). All such verification information must be:

- Retained by the Acquirer for a period of at least one year from the verification date; and
- Made available to Mastercard upon request.

6.2.2.2 Acquirer Authorization Monitoring Requirements

An Acquirer must implement real-time or near-real time alerts to monitor Merchant authorization messages on at least all of the following parameters:

- Number of authorization requests above a threshold set by the Acquirer for that Merchant
- An authorization approval rate that falls below a threshold set by the Acquirer for that Merchant
- Ratio of non-Card-read to Card-read Transactions that is above the threshold set by the Acquirer for that Merchant
- PAN key entry ratio that is above the threshold set by the Acquirer for that Merchant

- Repeated authorization requests for the same amount or the same Cardholder Account
- Ratio of technical fallback above a threshold set by the Acquirer for that Merchant
- Merchant authorization reversals that do not match a previous purchase Transaction
- Value of Merchant authorization refund that is above the threshold set by the Acquirer for that Merchant
- Out-of-pattern Transaction volume and/or velocity at a Merchant, Payment Facilitator, or ATM Terminal, including all of the following:
  - Repeated authorization requests
  - High velocity authorizations
  - Technical fallback of chip to magnetic stripe
  - High volume of Contactless Transactions
  - Sequential Account generated attacks
  - An abnormal increase in authorization requests received
  - An abnormal increase in the average Transaction amount
  - BIN attacks, defined as Account testing or highly unusual activity in connection with the use of Cards or Accounts issued under one or more BINs
  - An abnormally high number of authorization request responses indicating invalid PAN, CVC 1 or CVC 2 failure, invalid expiration date, incorrect PIN, Address Verification Service (AVS) mismatch, invalid Authorization Request Cryptogram (ARQC), or invalid Accountholder authentication value (AAV).
  - Transaction decline rate:
    - An excessive number of magnetic stripe Transactions occurring or attempted in a short period of time
    - An excessive number of ATM cash withdrawals occurring or attempted at the maximum cash withdrawal Transaction limit for that ATM in a short period of time

6.2.2.3 Acquirer Merchant Deposit Monitoring Requirements

A deposit is defined as a file of Transactions performed offline or online at a Merchant and submitted to the Merchant's Acquirer for payment. If deposit files are not used, the Acquirer should still monitor the total payment made to each Merchant.

Daily reports or real-time alerts monitoring Merchant deposits must be generated at the latest on the day following the deposit, and must be based on the following parameters:

- Increases in Merchant deposit volume
- Increase in a Merchant's average ticket size and number of Transactions for each deposit
- Change in frequency of deposits
- Change in technical fallback rates, or a technical fallback rate that exceeds five percent of a Merchant's total Transaction volume

  NOTE: Any report generated by the Acquirer relating to the investigation of a Merchant whose rate of technical fallback exceeds five percent of its total Transaction volume must be made available to Mastercard upon request.

- Force-posted Transactions (i.e., a Transaction that has been declined by the Issuer or the chip or any Transaction for which authorization was required but not obtained)

- Frequency of Transactions on the same Account, including credit (refund) Transactions
- Unusual number of credits, or credit dollar volume, exceeding a level of sales dollar volume appropriate to the Merchant category
- Large credit Transaction amounts, significantly greater than the average ticket size for the Merchant's sales
- Credit (refund) Transaction volume that exceeds purchase Transaction volume
- Credits issued by a Merchant subsequent to the Acquirer's receipt of a chargeback with the same PAN
- Credits issued by a Merchant to a PAN not previously used to effect a Transaction at the Merchant location
- Increases in Merchant chargeback volume

90-day Rule: Monitoring of Merchant Daily Volumes

The Acquirer must monitor the daily Transaction count and value at each Merchant in view of detecting abnormal or suspicious increase of Merchant activity.

To this effect, the daily Transactions count and value will be compared against the average daily Transaction count and amount for a period of at least 90 days, to lessen the effect of normal variances in a Merchant's business.

For a new Merchant, the Acquirer should set monitoring parameters to detect significant deviation from the Merchant's expected turnover as detailed in its business plan. The Acquirer may also compare the Merchant's average Transaction count and amount to those of other Merchants within the same MCC.

In the event that suspicious credit or refund Transaction activity is identified, if appropriate, the Acquirer should consider the suspension of Transactions pending further investigation.

6.2.2.4 Acquirer Channel Management Requirements

Mastercard requires Acquirers to monitor, on a regular basis, each parent Member ID/ICA number, child Member ID/ICA number, and individual Merchant, Payment Facilitator, and Staged Digital Wallet Operator in its Portfolio for the following:

- Total Transaction fraud basis points
- Domestic Transaction fraud basis points
- Cross-border Transaction fraud basis points (both Intraregional Transactions and Interregional Transactions)
- Fraud basis points at the parent Member ID/ICA level for the following:
  - Card-present Transactions
    - POS
    - Mobile POS (MPOS)
    - Cardholder-activated Terminal (CAT) (for example, CAT 1, CAT 2, and CAT 3)
  - Card-not-present (CNP) Transactions
    - E-commerce, including separate monitoring of non-authenticated, attempted authentication, and fully authenticated Transactions

- Mail order/telephone order (MO/TO)
- Recurring payment Transactions

6.2.2.5 3-D Secure Service Provider and Payment Gateway Monitoring

Requirements and Recommendations

Acquirers must implement fraud detection capabilities at any 3-D Secure Service Provider providing access to a 3-D Secure (3DS) server or Third Party Processor (TPP) performing payment gateway services to monitor all the following:

- Fraudulent attempts to connect to a 3DS server or payment gateway as a Merchant or Payment Facilitator (for example, a connection attempt from an unknown IP address or the use of an invalid credential)
- 3DS server or payment gateway Denial of Service (DoS) attack
- The authentication message flow indicating a PAN or BIN testing attack. This includes but is not limited to detection of (and capability to block) bot attacks using captcha, behavioral analytic tools or other available solutions. Bot attacks are defined as the use of automated web requests to test PANs through a 3DS Server payment gateway or more generally defined as web requests to manipulate, defraud, or disrupt a web site.
- Ensure Merchant names used in authentication messages match registered Merchant names
- Out-of-pattern number of single or multiple PAN Transactions associated to same customer account identifier or originating source (for example, the same email, telephone number, delivery address, browser fingerprint, or device identification number)

An Acquirer is recommended to implement fraud detection capabilities at 3DS Server payment gateways to monitor all the following:

- Receipt of confirmed fraud from Acquirers in view of creating a gray or negative listing of related IP and delivery address
- Additional monitoring recommendations and best practices as detailed in "Risk-based Authentication" section of the Mastercard Identity Check™ Program Guide

Upon detection of a 3DS Server payment gateway fraud attack by the Acquirer or upon notification from Mastercard of such an attack, the Acquirer must implement the necessary controls at the 3DS Server payment gateway to stop the attack within 72 hours (or within a timeframe approved by Mastercard) of detection or notification by Mastercard.

An Acquirer and its 3DS Server payment gateway must also analyze each attack to identify its modus operandi and implement corrective measures to prevent future attacks using the same technique(s).

6.2.2.6 Recommended Additional Acquirer Monitoring

Mastercard recommends that Acquirers additionally monitor the following parameters:

- Mismatch of Merchant name, MCC, Merchant ID, and/or Terminal ID
- Mismatch of e-commerce Merchant Internet Protocol (IP) addresses
- Transactions conducted at Merchant, Sponsored Merchants, and other entities registered in the Specialty Merchant Registration Program (refer to Chapter 9)

- Abnormal hours (i.e., outside of normal business hours) or seasons
- Sudden start of activity by an inactive/dormant Merchant (i.e., a Merchant that has not yet started to accept Cards or has ceased to accept Cards)
- Inconsistent authorization and clearing data elements for the same Transactions
- Mastercard *SecureCode*/Identity Check™ authentication rate
- Any Merchant exceeding the Acquirer's total Merchant average for fraud by 150 percent or more
  Geographic volume variances (i.e., abnormal increase of Merchant activity with some Issuer countries)
- Monitor the value, if any, returned in DE 48 subelement 84 (Merchant Advice Code) of authorization request response messages. An Acquirer is recommended to cease resending the same authorization request message when the MAC value is equal to 03 (Do Not Try Again) or 21 (Payment Cancellation).

6.2.2.7 Recommended Fraud Detection Tool Implementation

An Acquirer is recommended to implement a fraud detection tool that appropriately complements the fraud strategy deployed by the Acquirer. The combination of the authorization requirements, Merchant deposit monitoring requirements, and fraud detection tool should ensure that an Acquirer controls fraud to an acceptable level.

6.2.2.8 Ongoing Merchant Monitoring

An Acquirer must implement procedures for the conduct of periodic ongoing reviews of a Merchant's, Payment Facilitator's, or Staged Digital Wallet Operator's Transaction activity, for the purpose of detecting changes over time, including but not limited to:

- Monthly Transaction volume with respect to:
  - Total Transaction count and amount
  - Number of credit (refund) Transactions
  - Number of fraudulent Transactions
  - Average ticket size
  - Number of chargebacks and basis points
- Activity inconsistent with the Merchant's business model
- Transaction laundering
- Activity that is or may potentially be illegal or brand-damaging

As a best practice, Mastercard recommends that Acquirers use a Merchant monitoring solution for e-commerce Merchant activity so as to avoid processing illegal or brand-damaging Transactions.

For more information on ongoing Merchant monitoring requirements, refer to section 7.2.

6.2.2.9 Communicating Fraud and Chargeback Data to Merchants and Payment Facilitators

An Acquirer must be able, upon request from its Merchants and Payment Facilitators, to provide them with their fraud and chargeback data on a regular basis and at least monthly.

6.2.2.10 Fraud and Loss Control Internal Policies, Tracking, and Reporting Tools

Acquirers must establish internal policies, tracking and reporting tools covering all the following:

- Identification of individual Merchants and Payment Facilitators having a monthly average fraud, chargeback or decline rate exceeding thresholds set by the Acquirer, above which, an investigation of Merchant activities should be conducted to identify and implement any practices that require corrective actions. In all cases, these thresholds should be set to levels that maintain Merchant and payment facilitator compliance with Mastercard programs.
- Systematic investigation of any Standard violation by a Merchant, Payment Facilitator, Stage Digital Wallet Operator or ATM owner, either identified by the Acquirer or communicated by Mastercard. Each investigation must be followed by the identification and timely implementation of corrective actions to re-establish compliance with the Standards.

An Acquirer is recommended (unless mandated by Mastercard for a specific program) to create an internal report (the "investigation report") for each of the above events or exceeded thresholds and must include the following minimum information:

- Investigation number
- Investigation type
- Investigation date
- Detailed event description and analysis
- Description of the corrective actions
- Date the corrective action(s) was/were implemented
- Name of responsible person

6.2.2.11 Acquirer Recommendation to Report Suspected Fraud

An Acquirer is recommended to report Transactions to the Fraud and Loss Database that the Acquirer deems to be fraudulent as suspected fraud Transactions.

6.2.2.12 Acquirer Response to High Impact/Critical Fraud Alerts Raised by Issuers

An Acquirer approached by an Issuer with a High Impact/Critical Fraud management request is recommended to collaborate with the Issuer to the best of its ability.

Chapter 7 Merchant, Sponsored Merchant, and ATM Owner Screening and Monitoring Standards

This chapter may be of particular interest to Customer personnel responsible for screening and monitoring Merchants, Sponsored Merchants, and ATM owners.

7.1 Screening New Merchants, Sponsored Merchants, and ATM Owners

A Customer is responsible for verifying that a prospective Merchant, Sponsored Merchant, or ATM owner is conducting bona fide business operations as described in Rule 5.1.1, "Verify Bona Fide Business Operation", of the *Mastercard Rules* by performing the screening procedures set forth in this chapter.

The performance of these screening procedures does not relieve a Customer from the responsibility of following good commercial banking practices. The review of a credit report, an annual report, or an audited statement, for example, might suggest the need for further inquiry, such as additional financial and background checks regarding the business, its principal owners, and officers.

7.1.1 Required Screening Procedures

The Acquirer of a prospective Merchant or ATM owner, and any Payment Facilitator of the Acquirer with respect to a prospective Sponsored Merchant, must ensure that the following screening procedures are performed:

- In accordance with the Acquirer's "know your customer" policies and procedures implemented pursuant to Rule 1.2, "Mastercard Anti-Money Laundering and Sanctions Requirements", of the *Mastercard Rules*, collect information about the entity and each of its principal owners as necessary or appropriate for identification and due diligence purposes; verify that the information collected is true and accurate; and comply with all U.S. and local sanction screening requirements; and
- Confirm that the entity is located and conducting legal business in a country or territory within the Area of Use of the Acquirer's License, as described in Rule 5.4, "Merchant Location", and the *Mastercard Rules*; and
- Ensure that an inquiry is submitted to the Mastercard Alert to Control High-risk (Merchants) (MATCH™) system if a prospective Merchant or Sponsored Merchant proposes to accept Mastercard® Cards. If sales will be conducted on a website or digital application, the inquiry must include the uniform resource locator (URL) address. An Acquirer must submit inquiries both for its own Merchants and for the Sponsored Merchants of its Payment Facilitators; and
- Ensure Merchant names do not belong to other legal entities to prevent unlawful usage of existing business trademark, including impersonation of these names to scam consumers. Where legally allowed, controls include matching Merchant names with scam negative listing where they exist; and
- Ensure Merchant names that will be used in both authentication and authorization messages match (or is consistent with) registered Merchant names
- Establish fraud loss control measures appropriate for the business to be conducted, including but not limited to Transaction authorization and deposit activity monitoring parameters, as described in section 6.2.2, "Acquirer Fraud Loss Control Programs", of this manual; and

- Assign a Card acceptor business code (MCC) that most accurately describes the nature of the business (for MCC descriptions, see Chapter 3, "Card Acceptor Business Codes [MCCs]", of the *Quick Reference Booklet*).
- For a prospective negative option billing Merchant or Sponsored Merchant, identify any entity that provides service for the Merchant or Sponsored Merchant that would allow such entity to have access to Account data, and ensure that each such entity is registered with Mastercard as appropriate.

NOTE: A Customer must participate in the MATCH system unless excused by Mastercard or prohibited by law. If a Merchant or Sponsored Merchant is terminated for any of the reasons described in section 11.5.1, "Reason Codes for Merchants Listed by the Acquirer", the Acquirer must add the Merchant or Sponsored Merchant to the MATCH system.

7.1.2 Retention of Investigative Records

The Acquirer must retain all records concerning the investigation of a Merchant, Sponsored Merchant, or ATM owner for a minimum of two years after the date that the Merchant Agreement, Sponsored Merchant Agreement, or ATM Owner Agreement, as applicable, is terminated or expires. Such records may include any of the following, when applicable:

- Signed Merchant, Sponsored Merchant, or ATM Owner Agreement
- With respect to the screening of a Merchant or Sponsored Merchant, a statement from the Merchant about previous Merchant Agreements, including the names of the entities where the Merchant has or had the agreements and the reasons for terminating the agreements, if applicable
- Corporate or personal banking statements
- Report from a credit bureau, or, if the credit bureau report is incomplete or unavailable, the written results of additional financial and background checks of the business, its principal owners, and officers
- Site inspection report, to include photographs of premises, inventory verification, and the name and signature of the inspector of record
- Merchant or Sponsored Merchant certificate of incorporation, licenses, or permits
- Verification of references, including personal, business, or financial
- Verification of the authenticity of the supplier relationship for the goods or services (invoice records) that a Merchant or Sponsored Merchant is offering the Cardholder for sale
- Date-stamped MATCH inquiry records
- Date-stamped MATCH addition record
- All Customer correspondence with the Merchant, Sponsored Merchant, or ATM owner
- All correspondence relating to Issuer, Cardholder, or law enforcement inquiries concerning the Merchant, Sponsored Merchant, ATM owner, or any associated Service Provider
- Signed Service Provider contract, including the name of agents involved in the due diligence process
- Acquirer due diligence records concerning the Service Provider and its agents

Refer to Chapter 7, "Service Providers", of the *Mastercard Rules* manual for more information about Service Providers.

NOTE: Mastercard recommends that the Acquirer retain all records, in the event that Mastercard conducts an audit as necessary to verify compliance with the screening procedures described in this chapter.

7.1.3 Assessments for Noncompliance with Screening Procedures

Mastercard may audit an Acquirer for compliance with the screening procedures set forth in this chapter, and each Customer must comply with and assist any such audit. Mastercard will review the applicable records retained by the Acquirer to determine whether an Acquirer has complied with these screening procedures.

If Mastercard determines that an Acquirer has not complied with these screening procedures, and if the Acquirer does not correct all deficiencies that gave rise to the violation to the satisfaction of Mastercard within 30 days of knowledge or notice of such deficiencies, Mastercard may assess the Acquirer up to USD 100,000 for each 30-day period following the aforementioned period, with a maximum aggregate assessment of USD 500,000 during any consecutive 12-month period. Any such assessment(s) will be in addition to any other financial responsibility that the Acquirer may incur, as set forth in the Standards. Violators will also be subject to chargebacks of fraudulent Transactions.

Failure to inquire to the MATCH system as described in this chapter may result in an assessment of up to USD 5,000 for each instance of noncompliance.

7.2 Ongoing Monitoring

An Acquirer must monitor and confirm regularly that the Transaction activity of each of its Merchants (sales, credits, and chargebacks) is conducted in a legal and ethical manner and in full compliance with the Standards, and ensure that a Payment Facilitator conducts such monitoring with respect to each of its Sponsored Merchants, in an effort to deter fraud. Monitoring must focus on changes in activity over time, activity inconsistent with the Merchant's or Sponsored Merchant's business, or exceptional activity relating to the number of Transactions and Transaction amounts outside the normal fluctuation related to seasonal sales. Specifically for Mastercard POS Transaction processing, ongoing monitoring includes, but is not limited to, the Acquirer fraud loss controls relating to deposit (including credits) and authorization activity described in section 6.2.2.

With respect to an electronic commerce (e-commerce) Merchant, the Acquirer regularly, as reasonably appropriate in light of all circumstances, must review and monitor the Merchant's website(s) and business activities to confirm and to reconfirm regularly that any activity related to or using a Mark is conducted in a legal and ethical manner and in full compliance with the Standards. The Acquirer must ensure that a Payment Facilitator conducts such monitoring with respect to each of its Sponsored Merchant's website(s).

As a best practice, Mastercard recommends that Acquirers use a Merchant monitoring solution to review their e-commerce Merchants' and Sponsored Merchants' activity to avoid processing illegal or brand-damaging Transactions.

To mitigate social engineering fraud, Mastercard recommends that Acquirers in the Europe Region (excluding Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkey, Turkmenistan, Ukraine, and Uzbekistan) ensure that wallets detect typical fraud signals on wallet accounts, such as a high number of wallet top-ups or cryptocurrency purchases followed by rapid transfers to other digital wallets or cryptocurrency accounts, or by other spend with such wallets. It is recommended that Acquirers ensure that wallets apply strict criteria for blocking accounts and limit, for example, to a maximum of three, the number of Cards that can top-up an account.

An Acquirer must re-perform the onboarding screening procedures set forth in section 7.1.1 of this manual, in the following situations:

- Changes in ownership of a Merchant, Payment Facilitator, or ATM owner, whether confirmed or suspected
- Changes in country location of a Merchant, Payment Facilitator, or ATM owner
- Changes in Merchant or Payment Facilitator activities, declared by the Merchant, Payment Facilitator or detected by the Acquirer
- In case of suspected or confirmed violation of the Questionable Merchant Activity Program (QMAP), Business Risk Assessment Management (BRAM) Program, Excessive Fraud Merchant (EFM) and Excessive Chargeback Merchant (ECM) Program.

An Acquirer is recommended to re-perform, on a yearly basis, Merchant screening controls for Merchants with activities in the categories listed in section 9.1 of this manual.

7.3 Merchant Education

Once an acquiring relationship is established, an Acquirer must institute a fraud prevention program, including an education process consisting of periodic visits to Merchants, distribution of related educational literature, and participation in Merchant seminars. Instructions to Merchants must include Card acceptance procedures, use of the Electronic Warning Bulletin file or *Warning Notice*, authorization procedures including Code 10 procedures, proper completion of Transaction information documents (TIDs) (including primary account number [PAN] truncation), timely presentment of the Transaction to the Acquirer, and proper handling pursuant to Card capture requests. Customers must thoroughly review with Merchants the Standards against the presentment of fraudulent Transactions. In addition, Customers must review the data security procedures to ensure that only appropriate Card data is stored, magnetic stripe data never is stored, and any storage of data is done in accordance with the Standards for encryption, Transaction processing, and other prescribed practices.

An Acquirer must also ensure that a Payment Facilitator conducts appropriate education activities for each of its Sponsored Merchants.

7.4 Additional Requirements for Certain Merchant and Sponsored Merchant Categories

A Customer that acquires or proposes to acquire Transactions submitted by or on behalf of a Merchant, Sponsored Merchant, or other entity of a type listed in section 9.1 must comply with the registration and monitoring requirements of the Specialty Merchant Registration Program (SMRP) for each such Merchant, Sponsored Merchant, or other entity, as described in Chapter 9.

Chapter 8 Mastercard Fraud Control Programs

This chapter may be of particular interest to Customer personnel responsible for monitoring Merchant and/or Issuer activity for compliance with fraud loss control Standards.

8.1 Notifying Mastercard

This section describes the Merchant Fraud Control reporting requirements.

8.1.1 Acquirer Responsibilities

If an Acquirer has reason to believe that a Merchant with whom it has entered into a Mastercard Merchant Agreement is engaging in collusive or otherwise fraudulent or inappropriate activity, the Acquirer must immediately notify Franchise Customer Engagement & Performance by sending an email message to compliancereview@mastercard.com.

8.1.2 Issuer Responsibilities

If an Issuer becomes aware of any Merchant in violation of Rule 5.13 of the *Mastercard Rules* manual ("the Valid Transactions Rule"), through Cardholder complaints or otherwise, the Issuer immediately must notify Franchise Customer Engagement & Performance by sending an email message to compliancereview@mastercard.com.

8.2 Global Merchant Audit Program

Effective 15 October 2020, the Global Merchant Audit Program (GMAP) has been suspended until further notice.

8.3 Excessive Chargeback Program

Mastercard designed the Excessive Chargeback Program (ECP) to ensure that each Acquirer closely monitors, on an ongoing basis, its chargeback performance at the Merchant level. The ECP allows Mastercard to determine promptly when a Merchant has exceeded monthly ECP thresholds.

Refer to the Acquirer Chargeback Monitoring Program chapter of the *Data Integrity Monitoring Program* manual and the Pricing and Billing Resource Center on Mastercard Connect® for more information.

8.3.1 ECP Definitions

The following terms used in the ECP have the meanings set forth below.

Merchant

A Merchant (as the term "Merchant" is defined in Appendix E of this manual) is identified by the unique Acquirer-assigned Merchant identifier (MID) populated in DE 42 (Card Acceptor ID Code) in Transaction clearing messages.

Basis Points

Basis points are the number of chargebacks received by the Acquirer for a Merchant in a calendar month divided by the number of Mastercard Transactions in the preceding month acquired for that same Merchant and then multiplied by 10,000.

Excessive Chargeback Merchant (ECM)

An ECM is a Merchant that is identified as noncompliant in the ECM category of the Excessive Chargeback Merchant edit (Edit 2) as described in Chapter 8 of the *Data Integrity Monitoring Program* manual.

High Excessive Chargeback Merchant (HECM)

An HECM is a Merchant that is identified as noncompliant in the HECM category of the Excessive Chargeback Merchant edit (Edit 2) as described in Chapter 8 of the *Data Integrity Monitoring Program* manual.

8.3.2 Access and Monitoring Requirements

Acquirers of Merchants that exceed the ECM and HECM thresholds must monitor their Merchants through the Data Integrity Online application on Mastercard Connect®.

In addition, it is the Acquirer's responsibility on an ongoing basis to monitor each of its Merchants in accordance with the Standards, including but not limited to sections 6.2.2, 7.2, 7.3, and 7.4 of this manual.

Mastercard may assess an Acquirer of an ECM or HECM for noncompliance with the ECP as described in Edit 2 in Chapter 8 of the *Data Integrity Monitoring Program* manual.

8.3.3 Issuer Recovery

Mastercard will remit Issuer recovery fees to Issuers through the MCBS. Actual recovery will vary depending on the extent and duration of the violation and the number of chargebacks processed by each Issuer, and will be paid out of the amounts collected for the Issuer recovery fees described in Edit 2 in Chapter 8 of the *Data Integrity Monitoring Program* manual.

A USD 20 minimum threshold for the payment of Issuer recovery fees applies. An Issuer will receive a payment only if eligible to receive Issuer recovery fees of least USD 20. If no single Issuer meets the USD 20 minimum threshold, then the Issuer with the greatest burden will receive the full Issuer recovery amount collected from the Acquirer. If at least two Issuers have the same burden, then the funds will be split evenly between those Issuers.

8.3.4 Additional ECM and HECM Requirements

After a Merchant has been an ECM and/or HECM for six months (whether consecutive or non-consecutive), Mastercard may:

1. Advise the Acquirer with regard to the action plan and other measures that the Acquirer should take or consider taking to reduce the Merchant's Basis Points; and/or
2. Require the Acquirer to undergo a Franchise Management Program Customer Risk Review, at the Acquirer's expense, as described in Chapter 13 of this manual.

8.4 Questionable Merchant Audit Program (QMAP)

The Questionable Merchant Audit Program (QMAP) establishes minimum standards of acceptable Merchant behavior and identifies Merchants that may fail to meet such minimum standards by participating in collusive or otherwise fraudulent or inappropriate activity. The QMAP also permits an Issuer to obtain partial recovery of up to one-half of actual fraud losses, which total at least USD 2,000 in volume during the Case Scope Period resulting from fraudulent Transactions at a Questionable Merchant, based on Fraud and Loss Database reporting. The criteria to identify a Questionable Merchant and the fraud recovery process are described below.

8.4.1 QMAP Definitions

For purposes of the QMAP, the following terms have the meanings set forth below:

Cardholder bust-out account means an account for which all of the following conditions are true:

1. The Issuer closed the account prior to the earlier of (i) the Issuer requesting that Mastercard commence an investigation as to whether a Merchant is a Questionable Merchant, or (ii) Mastercard notifying the Issuer that Mastercard has commenced an investigation as to whether a Merchant is a Questionable Merchant; and
2. A Transaction arising from use of the account has not been charged back for either an authorization-related chargeback (as set forth in Chapter 2 of the Chargeback Guide) or fraud-related chargeback (as set forth in Chapter 2 of the Chargeback Guide) during the 180 days prior to the earlier of (i) the Issuer requesting that Mastercard commence an investigation as to whether a Merchant is a Questionable Merchant, or (ii) Mastercard notifying the Issuer that Mastercard has commenced an investigation as to whether a Merchant is a Questionable Merchant; and
3. At least one of the following is true:
    a. The account in question is "linked" to one or more Cardholder bust-out accounts. As used herein, to be "linked" means that personal, non-public information previously provided by an applicant in connection with the establishment of one or more Cardholder bust-out accounts (name, address, telephone number, social security number or other governmentissued identification number, authorized user, demand deposit account number, and the like) has been provided by an applicant in connection with the establishment of the subject account; or
    b. The account is linked to one or more Cardholder bust-out accounts used in Transactions with a Merchant that Mastercard identified as a Questionable Merchant in a Mastercard Announcement (AN) available on the Technical Resource Center on Mastercard Connect®; or
    c. The Cardholder requests that one or more additional persons be designated as an additional Cardholder of the account within a short period of time; or
    d. The Cardholder requests that the credit limit of the account be increased soon after the account is opened; or
    e. The Cardholder makes frequent balance queries or "open-to-buy" queries; or

f. No payment has been made of charges to the account; or
g. The Issuer closed the account after a failed payment (dishonored check or the like) of charges to the account.

Case Scope Period means the 120-calendar-day period preceding the date on which Mastercard commences an investigation into the activities of a suspected Questionable Merchant.

Questionable Merchant means a Merchant that satisfies all of the following criteria:

1. The Merchant submitted at least USD 50,000 in Transaction volume during the Case Scope Period;
2. The Merchant submitted at least five (5) Transactions to one or more Acquirers during the Case Scope Period; and
3. At least fifty (50) percent of the Merchant's total Transaction volume involved the use of Cardholder bust-out accounts
   OR

   At least three (3) of the following four (4) conditions apply to the Merchant's Transaction activity during the Case Scope Period:

   a. The Merchant's fraud-to-sales Transaction ratio was seventy (70) percent or greater.
   b. At least twenty (20) percent of the Merchant's Transactions submitted for authorization were declined by the Issuer or received a response of "01—Refer to issuer" during the Case Scope Period.
   c. The Merchant has been submitting Transactions for fewer than six (6) months.
   d. The Merchant's total number or total dollar amount of fraudulent Transactions, authorization declines, and Issuer referrals was greater than the Merchant's total number or total dollar amount of approved Transactions.

NOTE: Transaction activity ("on-us" or otherwise) that is not processed through Mastercard systems is not considered in determining whether a Merchant meets the criteria of a Questionable Merchant.

Mastercard has sole discretion, based on information from any source, to determine whether a Merchant meeting these criteria is a Questionable Merchant.

8.4.2 Mastercard Commencement of an Investigation

Mastercard, at its sole discretion, may commence a QMAP investigation of a Merchant. During the pendency of such an investigation, Mastercard may identify the Merchant being investigated in MATCH using MATCH reason code 00 (Questionable Merchant/Under Investigation).

Prior to 1 January 2022, if an Issuer has reason to believe that a Merchant may be a Questionable Merchant, the Issuer may notify Mastercard by either:

- Email message to qmap@mastercard.com
- Web-based form at https://form.mastercard.com/jfe/form/SV_01AtAPzF9FXjzrD

The QMAP Issuer Referral Form, completed by the Issuer, is available on **Mastercard Connect** > **Support** > **Form**.

Transactions that occurred during the Case Scope Period may qualify as eligible for recovery under the QMAP.

Effective 1 January 2022, if an Issuer has reason to believe that a Merchant may be a Questionable Merchant, the Issuer may notify Mastercard by web-based form at https://form.mastercard.com/jfe/form/SV_01AtAPzF9FXjzrD.

Transactions that occurred during the Case Scope Period may qualify as eligible for recovery under the QMAP.

In the notification, the Issuer must provide the basis for the Issuer's reason to believe that the Merchant may be a Questionable Merchant, and must provide all of the following information:

1. Issuer name and Member ID;
2. Acquirer name and Member ID;
3. Merchant name and address (city, state or province, and country);
4. Total number of Transactions conducted at the Questionable Merchant by the Issuer's Cardholders;
5. Total dollar volume of Issuer losses at the Questionable Merchant;
6. Percentage of Transactions attributed to Cardholder bust-out accounts, if applicable; and
7. Details of each Issuer-confirmed fraudulent Transaction, including Cardholder account number, Transaction date and time, and Transaction amount in U.S. dollars.

Mastercard may charge the Issuer a filing fee for each Merchant notification at the commencement of a QMAP investigation as described in section 8.4.9 of this manual.

If an Acquirer becomes aware that it is acquiring for a Questionable Merchant, the Acquirer must notify Mastercard promptly by email message at qmap@mastercard.com.

8.4.3 Mastercard Notification to Issuers

Mastercard will notify any impacted Issuers of its commencement of a QMAP investigation of a Merchant as follows, dependent upon whether the investigation concerns Cardholder bust-out accounts.

8.4.3.1 Investigations Concerning Cardholder Bust-out Accounts

If Mastercard commences a QMAP investigation concerning Cardholder bust-out accounts, Mastercard will notify an Issuer that Mastercard determines had accounts used in Transactions with the Merchant being investigated during the Case Scope Period.

The notification will be sent by email message to the Issuer's Security Contact then listed in the Company Contact Management application available on Mastercard Connect®. With the notification, Mastercard will provide details of Transactions arising from use of the Issuer's accounts at the Merchant during the Case Scope Period.

Within 60 days following such notice, an Issuer must report to the Fraud and Loss Database all fraudulent Transactions conducted during the Case Scope Period associated with the Merchant

being investigated. Transactions conducted on Cardholder bust-out accounts should be reported using fraud type code 51 (Bustout Collusive Merchant).

NOTE: To accelerate the determination by Mastercard of whether a Merchant is a Questionable Merchant, Issuers are urged to report fraudulent Transactions to the Fraud and Loss Database as expeditiously as feasible. For purposes of making such a determination, Mastercard only considers Transactions that take place (and the resulting fraudulent Transactions timely reported to the Fraud and Loss Database) during the Case Scope Period.

8.4.3.2 Investigations Not Concerning Cardholder Bust-out Accounts

If Mastercard commences a QMAP investigation not concerning Cardholder bustout accounts, Mastercard will notify an Issuer that Mastercard determines had accounts used in Transactions with the Merchant being investigated during the Case Scope Period only if Mastercard determines that the Merchant is a Questionable Merchant.

The notification will be sent by email message to the Issuer's Security Contact then listed in the Company Contact Management application available on Mastercard Connect®.

8.4.4 Mastercard Notification to Acquirers

Following the Mastercard evaluation of Transactions reported to the Fraud and Loss Database by Issuers, Mastercard will notify any Acquirer of the investigated Merchant that such Merchant has initially met the criteria of a Questionable Merchant. Such notification will be sent by email message to the Security Contact then listed for the Acquirer in the Company Contact Management application available on Mastercard Connect®.

Within 15 calendar days from the date of the Mastercard notification, the Acquirer may contest the Mastercard preliminary finding that a Merchant is a Questionable Merchant. In such an event, the Acquirer shall provide to Mastercard any supplemental information necessary to review the preliminary finding.

Mastercard has a right, but not an obligation, to audit an Acquirer's records for the purpose of attempting to determine whether a Merchant is a Questionable Merchant. An Acquirer must provide Mastercard such other or additional information as Mastercard may request to assist in the investigation.

The Acquirer must submit all documentation and records by email message to qmap@mastercard.com.

8.4.5 Merchant Termination

If the Acquirer determines that the Merchant under investigation (or any other of its Merchants) is a Questionable Merchant and terminates the Merchant Agreement for that reason, the Acquirer must add the Merchant to MATCH using MATCH reason code 08 (Mastercard Questionable Merchant Audit Program) within five (5) calendar days of the decision to terminate the Merchant.

8.4.6 Mastercard Determination

Mastercard will determine if a Merchant is a Questionable Merchant.

If Mastercard determines that the Merchant **is not** a Questionable Merchant, Mastercard will so notify each Issuer and Acquirer that provided information pertinent to the investigation. Such notice will be provided by email message to the Security Contact listed for the Customer in the Company Contact Management application available on Mastercard Connect®. In addition, Mastercard will delete the MATCH listing of the Merchant for MATCH reason code 00.

If Mastercard determines that the Merchant **is** a Questionable Merchant, Mastercard will:

1. Notify the Merchant's Acquirer, and
2. Identify the Merchant as a Questionable Merchant in a Mastercard Announcement for each of twelve (12) consecutive months, and
3. Modify the Merchant's MATCH record to reflect a reason code change from 00 (Under Investigation) to 20 (Mastercard Questionable Merchant Audit Program).

If the Acquirer terminates the Merchant Agreement because Mastercard determines the Merchant to be a Questionable Merchant, the Acquirer is required to identify the Merchant in MATCH with reason code 08 (Mastercard Questionable Merchant Audit Program).

8.4.7 Chargeback Responsibility

When Mastercard identifies a Questionable Merchant in a Mastercard Announcement, Mastercard will also specify a chargeback period ("start" and "end" dates) of at least one year. If an Acquirer continues to acquire from a Merchant after Mastercard declares the Merchant a Questionable Merchant, the Acquirer is responsible for valid chargebacks using message reason code 4849—Questionable Merchant Activity for a period of one year following publication of the Mastercard Announcement initially listing the Questionable Merchant; provided, Mastercard may extend the chargeback responsibility period. An Issuer has 120 days following the publication date of a Mastercard Announcement identifying a Questionable Merchant to charge back fraudulent Transactions that occur during the specified chargeback period to the Acquirer using reason code 4849—Questionable Merchant Activity.

8.4.8 Fraud Recovery

Following the identification of a Questionable Merchant in a Mastercard Announcement, and using data reported to the Fraud and Loss Database, Mastercard will notify any Issuer deemed by Mastercard to be eligible for partial recovery of loss due to fraudulent Transactions at a Questionable Merchant. The notice will disclose the amount of the recovery, less an administrative fee described in section 8.4.9, and the date that the amount will be credited to the Issuer's MCBS account.

An Issuer is not eligible to receive partial recovery of any Transaction:

1. For a Merchant not listed in the Mastercard Announcement, or
2. Taking place after the Mastercard Announcement date of publication, or
3. Not reported to Mastercard through the Fraud and Loss Database as described in section 8.4.3 of this manual, or

4. If the Issuer's total volume of reported fraudulent Transactions occurring at the Questionable Merchant during the Case Scope Period was less than USD 2,000, or
5. For which the Issuer received recovery through any existing remedy in the Mastercard system, including chargeback, recovery process, or the Issuer's own collection process, or
6. Performed with a Card with only magnetic stripe functionality.

Mastercard reserves the right to request additional information as a condition of determining whether a Transaction satisfactorily meets the eligibility requirements for Issuer partial recovery. In addition, Mastercard will not pay claims in excess of the amount collected from the Acquirer(s) for that purpose.

Mastercard will debit the fraud recovery amount from the Acquirer account and credit the Issuer account (less any administrative fee). Mastercard will process Issuer fraud recoveries according to MCBS.

8.4.9 QMAP Fees

Mastercard may charge an Issuer a filing fee of USD 500 for each Merchant that the Issuer has reason to believe is a Questionable Merchant and subsequently notifies Mastercard regarding such Merchant through email message at qmap@mastercard.com.

Mastercard may charge each Issuer an administrative fee equal to 15 percent of the Issuer recovery amount from a Questionable Merchant determination.

If Mastercard determines that a Merchant is a Questionable Merchant **and** the administrative fee is **equal to or more than** the filing fee, Mastercard will deduct the filing fee debited from the Issuer account at the commencement of the QMAP investigation from the administrative fee charged to the Issuer at the end of the QMAP investigation.

If Mastercard determines that a Merchant is a Questionable Merchant **and** the administrative fee is **less than** the Issuer filing fee, Mastercard may not debit an administrative fee from the Issuer account at the end of the QMAP investigation.

Mastercard may charge an Acquirer an audit fee not to exceed USD 2,500 for each identification of a Merchant as a Questionable Merchant.

8.6 Coercion Program

Mastercard developed the Coercion Program to help address Cardholder claims of being coerced into performing a Transaction.

For the purpose of this program, coercion is defined as Cardholder completion of a Transaction due to threatened or actual physical harm to the Cardholder (or the Cardholder's immediate family member) or the threatened or actual unlawful taking of property from the Cardholder (or the Cardholder's immediate family member).

8.6.1 Issuer Submissions

Prior to 1 January 2022, an Issuer may submit a Cardholder's claim of alleged coercion by providing the following documentation (in English or accompanied by an English translation) by either:

- Email message to coercion@mastercard.com
- Web-based form at https://form.mastercard.com/jfe/form/SV_6mvga8UpBcqRP3T
  Effective 1 January 2022, an Issuer may submit a Cardholder's claim of alleged coercion by providing the following documentation (in English or accompanied by an English translation) by web-based form at https://form.mastercard.com/jfe/form/SV_6mvga8UpBcqRP3T.
- A police report (if available)
  When a police report is not provided, the Cardholder's description must address why a police report was not provided. The Cardholder description must include whether an attempt was made to file a police report and, if not, why a police report was not filed.
- The Cardholder's detailed description of the alleged coercive event.
- The Coercion Claim Affidavit Form, completed by the Issuer on the Cardholder's behalf with the Cardholder's consent, thereby authorizing Mastercard to contact law enforcement regarding the alleged coercive event.
  The Coercion Claim Affidavit form is published on **Mastercard Connect** > **Support** > **Forms**.

8.6.2 Investigation Process

Mastercard will investigate a claim of alleged coercion when the following criteria are met:

- Within 120 calendar days from an alleged coercive event, Mastercard receives from two or more different issuers separate claims of alleged coerced Transactions performed by two or more unrelated Cardholders at the same Merchant location. The 120 calendar day period is calculated as 60 calendar days prior to and 60 calendar days after the date of the first alleged coerced Transaction. At Mastercard's sole discretion, the 120 calendar day period may be expanded.
- At least one claim of coercion includes a copy of a police report filed by the Cardholder
- The Transactions resulting from the alleged coercion were reported to the Fraud and Loss Database using fraud type code 00 (Lost Fraud) or 01 (Stolen Fraud). At Mastercard's sole discretion, a Transaction reported with a fraud reason code other than 00 or 01 may be included in the investigation.

Additionally, Mastercard will notify those Issuers whose Cardholders have performed a Transaction at the Merchant within the 120 calendar day (or longer) period of the alleged coerced event and who have not already submitted a Cardholder's claim of coercion that each Issuer has 10 calendar days from the initial notification date to contact the Cardholder, if necessary, and provide:

- A police report (if available) When a police report is not provided, the Cardholder's description must address why a police report was not provided. The Cardholder description

must include whether an attempt was made to file a police report and, if not, why a police report was not filed. • The Cardholder's detailed description of the alleged coercive event.

- The Coercion Claim Affidavit Form, completed by the Issuer on the Cardholder's behalf with the Cardholder's consent, thereby authorizing Mastercard to contact law enforcement regarding the alleged coercive event. The Coercion Claim Affidavit form is published on **Mastercard Connect** > **Support** > **Forms**.

8.6.3 Acquirer Responsibilities

Upon receiving a coercion investigation letter from coercion@mastercard.com, the Acquirer must:

- Immediately direct the Merchant to stop the coercive activity.
- Provide Mastercard with the information specified in the investigation letter and a resolution plan within 10 calendar days.

8.6.4 Investigation Results

Mastercard will notify the Issuer(s) and the Acquirer(s) involved in the investigation of the results by email from coercion@mastercard.com. The notification will advise that the investigation is closed and the claim of alleged coercion was:

- Not substantiated, or
- Substantiated.

The Issuer notification will also identify the Transactions eligible for chargeback and provide chargeback submission instructions.

The Acquirer notification will also advise the Acquirer of nonperformance with the Standards, identify the Transactions eligibl ck, and any nonperformance assessments to be billed.

8.6.5 Chargeback Responsibility

Chargebacks for confirmed coerced Transactions must use reason code 4849 (Questionable Merchant Activity) for Dual Message System transactions, and reason code 49 (Questionable Merchant Activity) for Debit Mastercard transactions processed on the Single Message System.

8.6.6 MATCH Reporting

Mastercard will add a Merchant to MATCH using reason code 24 (Illegal Transactions) when a merchant meets the Coercion Program criteria.

Mastercard will add a Merchant to MATCH using reason code of 00 (Questionable Acquirer/ Under Investigation) if the Merchant is identified in a subsequent claim of coercion within 12 months of meeting the Coercion Program criteria.

- If the subsequent claim of coercion is not confirmed to meet Coercion Program criteria, the MATCH record will be deleted.
- If the subsequent claim of coercion is confirmed to meet Coercion Program criteria, the MATCH record will be revised to reason code 24 (Illegal Transactions).

8.6.7 Franchise Management Program (FMP) Questionnaire-based Review

Completion of a Coercion Program FMP questionnaire:

- May be required by the Acquirer of a Merchant with two or more Coercion Program identifications within a 12-month period.
- Will be required by the Acquirer of a Merchant with three or more Coercion Program identifications within an 18-month period.

Questionnaire responses may be used as an escalation point by the Customer Engagement & and Performance Team to determine if an on-site FMP review is warranted. For information on the FMP, refer to Chapter 13 of this manual.

8.6.8 Coercion Program Performance Assessments

For the assessments that may apply for Coercion Program identifications, refer to section 1.1 Compliance with the Standards of this manual and Rule 2.1 Standards of the *Mastercard Rules* manual.

At its discretion, Mastercard may also include additional assessments for nonperformance with other Standards identified during the investigation including but not limited to an Acquirer's failure to inquire into MATCH before signing the Merchant.

8.7 Acceptor Business Code (MCC) Performance Program (Brazil Only)

The MCC Performance Program addresses Incomplete, Invalid, or Inappropriate MCC (as defined below) coding of Transactions. The MCC Performance Program may provide Issuer Interchange Recovery (for purposes of this Rule 8.7, "Issuer Interchange Recovery") as described in section 8.7.5.3 Issuer Interchange Recovery).

The program's current scope is limited to Brazil Domestic Transactions that are processed through the Global Clearing Management System (GCMS).

The Corporation has sole discretion to interpret and enforce the MCC Performance Program Standards.

8.7.1 Definitions

For purposes of the MCC Performance Program, the following terms have the meanings set forth below:

Case Scope Period

The 365-calendar day period preceding the date on which Mastercard commences an investigation into the activities of a suspected Qualifying Merchant. Transactions that occurred before the program effective date of 14 May 2021 will be excluded.

An Incomplete, Invalid or Inappropriate MCC

An MCC which:

1. Is reserved for future use in the *Quick Reference Booklet*; or
2. Is missing numerical characters; or
3. Does not describe the Merchant's primary business or does not conform to the *Mastercard Rules*, Rule 5.8.1 Acceptor Business Code (MCC) Information

Qualifying Merchant

A Brazil-based Merchant, Payment Facilitator, or Staged Digital Wallet Operator that has submitted at least BRL 250,000 in Transaction Volume and ten Transactions for processing through GCMS with an Incomplete, Invalid or Inappropriate MCC during the Case Scope Period.

8.7.2 Notifying Mastercard

If an Issuer has reason to believe that a First Presentment/1240 message may contain an Incomplete, Invalid or Inappropriate MCC, the Issuer may notify the Corporation by e-mail message to MCC_Performance@mastercard.com.

In the notification, the Issuer must provide all the following information:

1. Issuer Name
2. Issuer ICA
3. Merchant ID (MID) present in Data Element (DE) 42 (Card Acceptor ID Code) of the First Presentment/1240 message
4. Merchant name and location present in DE 43 (Card Acceptor Name/Location) and its subfields of the First Presentment/1240 message
5. When applicable, the three-digit Wallet Identification Number (WID) assigned to the Staged DWO in PDS 0207 of the First Presentment/1240 messages
6. When applicable, the Payment Facilitator ID present in DE 48, subelement 37, subfield 1 (Payment Facilitator ID) of the First Presentment/1240 message
7. The MCC present in DE 26 (Card Acceptor Business Code [MCC]) of the First Presentment/1240 message
8. The Tax ID number present in DE 112 (Additional Data [National Use]), subelement 012 (Brazil Commercial and Financing Data) of the First Presentment/1240 message
9. The Issuer's explanation in English, or accompanied by an English translation, as to why the Issuer believes the MCC present in the First Presentment/1240 message is alleged to be an Incomplete, Invalid, or Inappropriate MCC
10. The Issuer's explanation in English, or accompanied by an English translation, as to what the Issuer believes to be the appropriate MCC and why the Issuer believes that MCC to be appropriate

Mastercard may initiate an MCC miscoding investigation without Issuer notification.

8.7.3 Mastercard Notification to Acquirers

If Mastercard determines that an entity may be a Qualifying Merchant, Mastercard will notify the Acquirer by e-mail message from MCC_Performance@mastercard.com to the Acquirer's Security Contact as listed in the My Company Manager application on Mastercard Connect®. If a Security Contact is not listed, the notification will be sent to the Principal Contact.

Within 30 calendar days from the date of the Mastercard notification e-mail, the Acquirer may:

- Advise Mastercard that the MCC assigned to the Qualifying Merchant has been changed; or
- Provide an explanation and/or documentation (in English or accompanied by an English translation) that the entity is not a Qualifying Merchant (meaning the MCC present in the First Presentment/1240 message is appropriate). The Acquirer must submit all documentation by e-mail message to MCC_Performance@mastercard.com.

8.7.4 Mastercard Determination

Mastercard will notify the Issuer(s) and the Acquirer(s) involved in the investigation of the results by email from MCC_Performance@mastercard.com to the Security Contact as listed in the My Company Manager application on Mastercard Connect®. If a Security Contact is not listed, the notification will be sent to the Principal Contact. The notification will advise that the investigation is closed, and the Issuer's claim was:

- Not substantiated. If not substantiated, the notification will include information on the Issuer Filing Fee.
- Substantiated. If substantiated, the notification will include information on the applicable assessments, recovery amounts, and fees.

8.7.5 Assessments, Recovery Amounts, and Fees

There are three components to assessments, recovery amounts, and fees:

- Issuer Filing Fee
- Acquirer Non-Performance Assessments
- Issuer Interchange Recovery (collected from the Acquirer(s) and credited to the Issuer(s))

8.7.5.1 Issuer Filing Fee

If Mastercard determines that a claim is not substantiated, Mastercard will bill each reporting Issuer a filing fee of BRL 25,000 per Merchant, Payment Facilitator, or Staged Digital Wallet Operator.

8.7.5.2 Acquirer Non-Performance Assessments

Mastercard may bill an Acquirer for non-performance assessments for each impacted Merchant ID (MID) for a substantiated claim as described in the table below:

Miscoded Brazil GCMS Domestic Transaction Volume	Non-Performance Assessment
Less than BRL 5,000,000	Up to BRL 10,000
More than BRL 5,000,000 but less than BRL 30,000,000	Up to BRL 50,000
More than BRL 30,000,000	Up to BRL 150,000

Non-performance assessments may be escalated as described in the below tables.

For the second violation within twelve months:

Miscoded Brazil GCMS Domestic Transaction Volume	Non-Performance Assessment
Less than BRL 5,000,000	Up to BRL 20,000
More than BRL 5,000,000 but less than BRL 30,000,000	Up to BRL 100,000
More than BRL 30,000,000	Up to BRL 300,000

For the third violation within twelve months:

Miscoded Brazil GCMS Domestic Transaction Volume	Non-Performance Assessment
Less than BRL 5,000,000	Up to BRL 30,000
More than BRL 5,000,000 but less than BRL 30,000,000	Up to BRL 150,000
More than BRL 30,000,000	Up to BRL 450,000

For the fourth and subsequent violations within twelve months:

Miscoded Brazil GCMS Domestic Transaction Volume	Non-Performance Assessment
Less than BRL 5,000,000	Up to BRL 40,000

Miscoded Brazil GCMS Domestic Transaction Volume	Non-Performance Assessment
More than BRL 5,000,000 but less than BRL 30,000,000	Up to BRL 200,000
More than BRL 30,000,000	Up to BRL 600,000

Acquirer Non-Performance Assessments may be mitigated at the Corporation's discretion, using the below guidance:

- Mitigated by 50% if the Qualifying Merchant is recoded with an appropriate MCC within 5 calendar days of the Corporation's notification.
- Mitigated by 25% if the Qualifying Merchant is recoded with an appropriate MCC within fifteen calendar days of the Corporation's notification.

8.7.5.3 Issuer Interchange Recovery (Collected from the Acquirer(s) and Credited to the Issuers(s))

Mastercard will calculate and assess Acquirers for Issuer Interchange Recovery by applying adjustments to the interchange rate submitted for each Transaction processed through GCMS within a substantiated claim. The interchange adjustment will be made based on the calculated differential between the interchange rates submitted for each Transaction processed through GCMS within a substantiated claim and the interchange rates that should have been submitted based on the validity or accuracy of the MCC data, at the product level.

In instances where the Acquirer is unable to identify the appropriate MCC or fails to recode the Qualifying Merchant with an appropriate MCC within the required time frame, Mastercard may calculate the interchange adjustment based on the differential between the interchange rate submitted for each Transaction processed through GCMS within a substantiated claim and the highest Brazil interchange rates by product.

Mastercard will debit each responsible Acquirer the Issuer Interchange Recovery amount for each substantiated claim and credit each impacted Issuer through the settlement process for each substantiated claim.

Actual recovery provided to each impacted Issuer will vary depending on the extent and duration of the violation, the number of Transactions and Transaction Volume processed through GCMS by each Issuer, and will be paid solely out of the amounts Mastercard collects from the responsible Acquirer(s) for the Issuer Interchange Recovery amount.

Chapter 9 Mastercard Registration Program

This chapter may be of particular interest to Customer personnel responsible for registering Merchants, Submerchants, and other entities with Mastercard. The Mastercard Registration Program (MRP) formerly was referred to as the Merchant Registration Program.

9.1 Specialty Merchant Registration Program Overview

Mastercard requires Customers to register the following Merchant types, including Sponsored Merchants, and other entities using the Specialty Merchant Registration Program system, available through Mastercard Connect®:

- Non-face-to-face adult content and services Merchants—Card acceptor business codes (MCCs) 5967 and 7841 (refer to section 9.4.1)
- Non–face-to-face gambling Merchants—MCCs 7801, 7802, and 7995 (refer to section 9.4.2)

  For a non-face-to-face gambling Merchant located in the U.S. Region, the Customer must submit the required registration items as described in section 9.4.2 to Mastercard by sending an email message to specialty_merchant_registration@mastercard.com.
- Non–face-to-face pharmaceutical Merchants—MCCs 5122 and 5912 (refer to section 9.4.3)
- Non–face-to-face tobacco product Merchants—MCC 5993 (refer to section 9.4.3)
- Government-owned lottery Merchants (U.S. Region only)—MCC 7800 (refer to section 9.4.4)

  For a government-owned lottery Merchant located in the U.S. Region, the Customer must submit the required registration items as described in section 9.4.4 to Mastercard by sending an email message to specialty_merchant_registration@mastercard.com.
- Government-owned lottery Merchants (Global, Excluding U.S. Region)—MCC 9406 (refer to section 9.4.4)
- Skill games Merchants—MCC 7994 (refer to section 9.4.5)

  For a skill games Merchant located in the U.S. Region (or outside the U.S. Region in order to use MCC 7994 to identify Transactions involving U.S. Region-issued Accounts), the Customer must submit the required registration items as described in section 9.4.5 to Mastercard by sending an email message to specialty_merchant_registration@mastercard.com.
- High-risk cyberlocker Merchants—MCC 4816 (refer to section 9.4.6)
- Recreational cannabis Merchants (Canada Region only)—regardless of MCC (refer to section 9.4.7)
- High-risk securities Merchants—MCC 6211 (refer to section 9.4.8)
- Cryptocurrency Merchants—MCC 6051 (refer to section 9.4.9)
- Negative option billing Merchants selling physical products—MCC 5968 (refer to section 9.4.10)

During registration, the Acquirer must provide each website uniform resource locator (URL) from which Transactions as described in this section may arise, whether the website is that of a Merchant, Sponsored Merchant, or other entity. With respect to Transactions submitted by a Staged Digital Wallet Operator (DWO), each individual website URL at which Transactions as described in this section may be effected must be individually registered.

If a Customer acquires Transactions for any of the Merchant types listed herein without first registering the Merchant, Sponsored Merchant, or other entity in accordance with the Standards described in this section, Mastercard may assess the Customer as set forth in section 9.2.1 of this manual. In addition, the Acquirer must ensure that the violation is corrected promptly.

Refer to the *Mastercard Registration Program User Manual* for directions for completing registration tasks available in the MRP system.

9.2 General Registration Requirements

The Customer must provide all of the information requested for each Merchant, Sponsored Merchant, or other entity required to be registered through the MRP system. For each such entity, the requested information includes:

- The name, doing business as (DBA) name, and address
- The central access phone number or customer service phone number, website URL, or email address
- The name(s), address(es), and tax identification number(s) (or other relevant national identification number) of the principal owner(s)
- A detailed description of the service(s), product(s), or both that the entity will offer to Cardholders
- A description of payment processing procedures, Cardholder disclosures, and other practices including, but not limited to:
  - Data solicited from the Cardholder
  - Authorization process (including floor limits)
  - Customer service return policies for card transactions
  - Disclosure made by the Merchant before soliciting payment information (including currency conversion at the Point of Interaction [POI])
  - Data storage and security practices
- The identity of any previous business relationship(s) involving the principal owner(s) of the entity
- A certification, by the officer of the Customer with direct responsibility to ensure compliance of the registered entity with the Standards, stating that after conducting a diligent and good faith investigation, the Customer believes that the information contained in the registration request is true and accurate

Only Mastercard can modify or delete information about a registered entity. Customers must submit any modification(s) about a registered entity in writing to Mastercard, with an explanation for the request. Mastercard reserves the right to deny a modification request.

Customers should send any additional requested information and modification requests by email message to specialty_merchant_registration@mastercard.com.

For requirements specific to Merchants that are required to implement the Mastercard Site Data Protection (SDP) Program, refer to section 2.2 of this manual.

9.2.1 Merchant Registration Fees and Noncompliance Assessments

Mastercard assesses the Acquirer an annual USD 500 registration fee for each Merchant and Sponsored Merchant under the categories listed in section 9.1. Mastercard will collect the fee from the Acquirer through the Mastercard Consolidated Billing System (MCBS).

Mastercard may assess a Customer that acquires Transactions for any of these Merchant or Sponsored Merchant types without first registering the Merchant in accordance with the requirements of the MRP. A violation will result in an assessment of up to USD 10,000.

If, after notice by Mastercard of the Acquirer's failure to register a Merchant or Sponsored Merchant, that Acquirer fails to register its Merchant within 10 days of notice, the Acquirer will be subject to additional assessments of USD 5,000 per month for up to three months, and USD 25,000 per month thereafter, until the Acquirer satisfies the requirement. In addition, the Acquirer must ensure that the violation is corrected promptly. Such Merchant or Sponsored Merchant may also be deemed by Mastercard, in its sole discretion, to be in violation of Rule 5.11.7 of the *Mastercard Rules* manual ("the Illegal or Brand-damaging Transactions Rule").

9.3 General Monitoring Requirements

The monitoring requirements described in this section apply to Customers that acquire non-face-to-face adult content and services Transactions, non–face-to-face gambling Transactions, non–face-to-face pharmaceutical and tobacco product Transactions, government-owned lottery Transactions, skill games Transactions, certain cyberlocker Transactions, recreational cannabis Transactions (Canada Region only), certain securities Transactions, cryptocurrency Transactions, or negative option billing Transactions:

- The Acquirer must ensure that each such Merchant implements real-time and batch procedures to monitor continually all of the following:
  - Simultaneous multiple Transactions using the same Account number
  - Consecutive or excessive attempts using the same Account number

  When attempted fraud is evident, a Merchant should implement temporary bank identification number (BIN) blocking as a fraud deterrent.
- The Acquirer must ensure that each such Merchant complies with the fraud control Standards in Chapter 6 of this manual.

9.4 Additional Requirements for Specific Merchant Categories

Customers should review thoroughly these additional requirements for specific Merchant categories.

9.4.1 Non-face-to-face Adult Content and Services Merchants

A non-face-to-face adult content and services Transaction occurs when a consumer uses an Account in a Card-not-present environment to purchase adult content or services, which may include but is not limited to subscription website access; streaming video; pictures and images; and videotape and DVD rentals and sales.

An Acquirer must identify all non-face-to-face adult content and services Transactions using one of the following MCC and Transaction category code (TCC) combinations, as appropriate:

- MCC 5967 (Direct Marketing—Inbound Telemarketing Merchants) and TCC T; or
- MCC 7841 (Video Entertainment Rental Stores) and TCC T.

Before an Acquirer may process non-face-to-face adult content and services Transactions from a Merchant or Sponsored Merchant, it must register the Merchant or Sponsored Merchant with Mastercard as described in section 9.2 of this manual.

By registering an adult content and services Merchant or Sponsored Merchant, the Acquirer is certifying that the Merchant or Sponsored Merchant meets the following requirements and has effective controls in place to monitor, block, and where necessary, take down all content as appropriate. All of the following Merchant requirements also apply to Sponsored Merchants.

In situations where the Merchant allows a third-party user ("content provider") to upload or generate content, including real-time/live streaming content:

1. The Merchant must enter into a written agreement with each content provider and such written agreement must:
   a. Specifically prohibit any activity that is illegal or otherwise violates the Standards
   b. Require the content provider to obtain and keep on record written consent from all persons depicted in the content specific to the following areas:
      – Consent to be depicted in the content
      – Consent to allow for the public distribution of the content and to upload the content to the Merchant's website
      – If the content will be made available for downloading by other users, consent to have the content downloaded
   c. Require the content provider to verify the identity and age of all persons depicted in content to ensure that all persons depicted are adults and to be able to provide supporting documents upon request.
2. The Merchant must only permit content uploads from verified content providers and must have a robust process for verifying the age and identity of the content provider, which includes the review and validation of a government-issued identification and steps to ensure that the government identification is in the possession of, and belongs to, the content provider. The use of a third-party vendor that specializes in the validation of government identifications is recommended.
3. All uploaded content must be reviewed prior to publication to ensure that the content is not illegal and does not otherwise violate the Standards.
4. If providing real-time or live video streaming services, the Merchant must operate on a platform that the Merchant is able to fully control and that allows for real-time monitoring and the removal of the content being streamed.

For all adult content and services Merchants:

1. The Merchant must not market the content of its website or permit content search terms to give the impression that the content contains child exploitation materials or the depiction of nonconsensual activities.
2. The Merchant must support a complaint process that allows for the reporting of content that may be illegal or otherwise violates the Standards and must review and resolve all

reported complaints within seven (7) business days. In the event that such review yields evidence of illegal content, the Merchant must remove that content immediately.

3. The Merchant must offer the ability for any person depicted in a video or other content to appeal to remove such content. Once triggered, the Merchant must, through a reasonable process, confirm that the appropriate consent was obtained, including as required above. If consent cannot be established, or if the person depicted in the content can demonstrate that the consent is void under applicable law, the Merchant must remove the content with immediate effect. If the Merchant disagrees that consent is void under applicable law, the Merchant must allow such disagreement to be resolved by a neutral body, at the Merchant's expense.
4. The Merchant must provide its Acquirer with monthly reports that include a list of all content, including URLs and videos, flagged as potentially illegal or otherwise in violation of the Standards and the relevant actions taken by the Merchant, as well as details of all complaints and take-down requests the Merchant received. The Acquirer must share these reports with Mastercard, upon request.
5. The Merchant must not attract users to its website by utilizing adult content that is illegal or otherwise violates the Standards.
6. The Merchant must have effective policies in place that prohibit the use of its website in any way that promotes or facilitates human trafficking, sex trafficking or physical abuse. Active membership and participation in an anti-human trafficking and/or anti-child exploitation organization is highly recommended.
7. Upon request, the Acquirer must be able to provide Mastercard with temporary account credentials that allow access to a Merchant website for up to seven (7) days to view all content that is behind a paywall or otherwise restricted to members of the website.

9.4.2 Non–face-to-face Gambling Merchants

A non–face-to-face gambling Transaction occurs in a Card-not-present environment when a consumer uses an Account to place a wager or purchase chips or other value usable for gambling provided by a wagering or betting establishment as defined by MCC 7801 (Internet Gambling), MCC 7802 (Government Licensed Horse/Dog Racing), or MCC 7995 (Gambling Transactions).

Before acquiring Transactions or Gaming Payment Transactions reflecting non–face-to-face gambling, an Acquirer first must register the Merchant, Sponsored Merchant, or other entity with Mastercard as described in section 9.2.

An Acquirer must identify all non–face-to-face gambling Transactions using MCC 7995 and TCC U unless the Acquirer has also registered the Merchant, Sponsored Merchant, or other entity as described below, in which case the Acquirer may use MCC 7801 or 7802 instead of MCC 7995.

An Acquirer that has registered a U.S. Region Merchant, Sponsored Merchant, or other entity engaged in legal gambling activity involving sports intrastate Internet gambling must identify all non-face-to-face gambling Transactions arising from such Merchant, Sponsored Merchant, or other entity with MCC 7801 and TCC U.

Gaming Payment Transactions must be identified as described in the Mastercard Gaming and Gambling Payment Program Standards.

In addition to the requirement to register the Merchant, Sponsored Merchant, or other entity as described in section 9.2, an Acquirer registering a U.S. Region Merchant, Sponsored Merchant, or other entity engaged in legal gambling activity involving horse racing, dog racing, sports intrastate Internet gambling, or non-sports intrastate Internet gambling must demonstrate that an adequate due diligence review was conducted by providing the following items via email to Mastercard at specialty_merchant_registration@mastercard.com as part of the registration process (herein, all references to a Merchant also apply to a Sponsored Merchant or other entity):

1. **Evidence of legal authority.** The Acquirer must provide:
   - a copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority, that expressly authorizes the Merchant to engage in the gambling activity; and
   - any law applicable to the Merchant that permits the gambling activity.
2. **Legal opinion.** The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a reputable private sector U.S. lawyer or U.S. law firm purporting to have expertise in the subject matter. The legal opinion must:
   - identify all relevant gambling, gaming, and similar laws applicable to the Merchant;
   - identify all relevant gambling, gaming, and similar laws applicable to Cardholders permitted by the Merchant to transact with the Merchant; and
   - demonstrate that the Merchant's and Cardholders' gambling and payment activities comply at all times with any laws identified above.

   The Acquirer must provide Mastercard with a copy of such legal opinion. The legal opinion must be acceptable to Mastercard.
3. **Effective controls.** The Acquirer must provide certification from a qualified independent third party demonstrating that the Merchant's systems for operating its gambling business:
   - include effective age and location verification; and
   - are reasonably designed to ensure that the Merchant's Internet gambling business will remain within legal limits (including in connection with interstate Transactions).

   The certification must include all screenshots relevant to the certification (for example, age verification process). Certifications from interested parties (such as the Acquirer, Independent Sales Organizations [ISOs], the Merchant, and so on) are not acceptable substitutes for the independent third-party certification.
4. **Notification of changes.** The Acquirer must certify that it will notify Mastercard of any changes to the information that it has provided to Mastercard, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to Mastercard (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.
5. **Acceptance of responsibilities.** The Acquirer must specifically affirm that it will not submit restricted Transactions from the Merchant for authorization.

Mastercard must approve the registration request before the Acquirer may process any non-face-to-face gambling Transactions for the U.S. Region Merchant, Sponsored Merchant, or other entity.

9.4.3 Pharmaceutical and Tobacco Product Merchants

A non–face-to-face pharmaceutical Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase prescription medicines from a Merchant whose primary business is non–face-to-face selling of prescription drugs.

A non–face-to-face tobacco product Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase tobacco products (including, but not limited to cigarettes, cigars, loose tobacco, or electronic nicotine delivery systems [such as electronic cigarettes {e-cigarettes}]) from a Merchant whose primary business is non-face-to-face selling of tobacco products.

Before acquiring Transactions as described below, an Acquirer first must register the Merchant with Mastercard as described in section 9.2:

- Non–face-to-face sale of pharmaceuticals (MCC 5122 and MCC 5912)
- Non–face-to-face sale of tobacco products (MCC 5993)

An Acquirer must identify all non-face-to-face pharmaceutical Transactions using MCC 5122 (Drugs, Drug Proprietors, and Druggists Sundries) and TCC T for wholesale purchases or MCC 5912 (Drug Stores, Pharmacies) and TCC T for retail purchases. An Acquirer must identify all non-face-to-face tobacco product Transactions using MCC 5993 (Cigar Stores and Stands) and TCC T.

For clarity, the term acquiring, as used in this section, is "acquiring Activity" as such term is used in Rule 2.3 of the *Mastercard Rules* manual.

At the time of registration of a Merchant or Sponsored Merchant in accordance with this section, the Acquirer of such Merchant or Sponsored Merchant must have verified that the Merchant's or Sponsored Merchant's activity complies fully with all laws applicable to Mastercard, the Merchant or Sponsored Merchant, the Issuer, the Acquirer, and any prospective customer of the Merchant or Sponsored Merchant. Such verification may include, but is not limited to, a written opinion from independent, reputable, and qualified legal counsel or accreditation by a recognized third party.

By registering a Merchant or Sponsored Merchant as required by this section, the Acquirer represents and warrants that the Acquirer has verified compliance with applicable law as described above. The Acquirer must maintain such verification for so long as it acquires Transactions from the Merchant or Sponsored Merchant that is subject to the aforedescribed registration requirement and must, no less frequently than every 12 months, confirm continued compliance with applicable law concerning the business of the registered Merchant or Sponsored Merchant. The Acquirer must furnish Mastercard with a copy of such documentation promptly upon request.

9.4.4 Government-owned Lottery Merchants

The following requirements apply to government-owned lottery Merchants in the U.S. Region (see section 9.4.4.1) and government-owned lottery Merchants in the Asia/Pacific, Canada, Europe, Latin America and the Caribbean, and Middle East/Africa Regions (see section 9.4.4.2),

respectively, including Merchants initiating Gaming Payment Transactions pursuant to the Mastercard Gaming and Gambling Payment Program Standards.

9.4.4.1 Government-owned Lottery Merchants (U.S. Region Only)

A U.S. Region Acquirer must:

- use MCC 7800 (Government Owned Lottery [U.S. Region Only]) to identify Transactions arising from a U.S. Region Merchant, Sponsored Merchant, or other entity and involving the purchase of a state lottery ticket; and
- register each such Merchant, Sponsored Merchant, or other entity with Mastercard as described in section 9.2 and this section 9.4.4.1.

To register a Merchant, Sponsored Merchant, or other entity, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items via email to Mastercard at specialty_merchant_registration@mastercard.com as part of the registration process (herein, all references to a Merchant also apply to a Sponsored Merchant or other entity):

1. **Evidence of legal authority.** The Acquirer must provide:
   - a copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority, that expressly authorizes the Merchant to engage in the gambling activity; and
   - any law applicable to the Merchant that permits state lottery ticket sales.
2. **Legal opinion.** The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a private sector U.S. lawyer or U.S. law firm. The legal opinion must:
   - identify all relevant state lottery and other laws applicable to the Merchant;
   - identify all relevant state lottery and other laws applicable to Cardholders permitted by the Merchant to transact with the Merchant; and
   - demonstrate that the Merchant's and Cardholders' state lottery and payment activities comply at all times with any laws identified above.

   The Acquirer must provide Mastercard with a copy of such legal opinion. The legal opinion must be acceptable to Mastercard.
3. **Effective controls.** The Acquirer must provide certification from a qualified independent third party demonstrating that the Merchant's systems for operating its state lottery business:
   - include effective age and location verification; and
   - are reasonably designed to ensure that the Merchant's state lottery business will remain within legal limits (including in connection with interstate Transactions).

   The certification must include all screenshots relevant to the certification (for example, age verification process). Certifications from interested parties (such as the Acquirer, ISOs, the Merchant, and so on) are not acceptable substitutes for the independent third-party certification.
4. **Notification of changes.** The Acquirer must certify that it will notify Mastercard of any changes to the information that it has provided to Mastercard, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include

any revisions or additions to the information provided to Mastercard (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.

5. **Acceptance of responsibilities.** The Acquirer must specifically affirm that it will not submit restricted Transactions from the Merchant for authorization.

Mastercard must approve the registration request before the Acquirer may process any government-owned lottery Transactions for the Merchant, Sponsored Merchant, or other entity.

9.4.4.2 Government-owned Lottery Merchants (Global, Excluding U.S. Region)

An Acquirer may use MCC 9406 (Government Owned Lottery [Global, Excluding U.S. Region]) to identify a Merchant, Sponsored Merchant, or other entity located in the Asia/Pacific, Canada, Europe, Latin America and the Caribbean, or Middle East/Africa Region that is engaged in the sale of lottery tickets, recurring lottery subscriptions, or both. For lottery entities located in the U.S. Region, refer to section 9.4.4.1. For lottery entities located in any other country, refer to section 9.4.2.

Subject to applicable law and regulation, a government-administered lottery scheme may sell lottery tickets or lottery subscription services through the Internet. As set forth in section 9.2 above, an Acquirer must register any Merchant, Sponsored Merchant, or other entity conducting such sale in a non-face-to-face environment.

For the avoidance of doubt, this registration requirement extends to any agent duly licensed by the appropriate government authority to sell lottery tickets online.

9.4.5 Skill Games Merchants

A skill games Transaction occurs when a consumer uses an Account to participate in certain games (herein, "skill games"). For purposes of this section, "skill games" means:

- Game participants pay a game entry fee;
- The outcome of the game is determined by the skill of the participants rather than by chance;
- The winner of a game receives cash and/or a prize of monetary value; and
- No non-participant in the game pays or receives cash and/or a prize of monetary value in relation to the game.

An Acquirer:

- May use MCC 7994 (Video Game Arcades/Establishments) to identify Transactions arising from:
  - A U.S. Region Merchant, Sponsored Merchant, or other entity conducting skill games; or
  - A Merchant, Sponsored Merchant, or other entity located outside the U.S. Region conducting skill games that accepts payment from a consumer using a U.S. Region Account for participation in a skill game conducted by such Merchant, Sponsored Merchant, or other entity;

AND

- Must register the Merchant, Sponsored Merchant, or other entity with Mastercard as described in section 9.2 and this section 9.4.5 (including any U.S. Region Merchant proposing to conduct Gaming Payment Transactions).

To register a Merchant, Sponsored Merchant, or other entity, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items via email to Mastercard at specialty_merchant_registration@mastercard.com as part of the registration process (herein, all references to a Merchant also apply to a Sponsored Merchant or other entity):

1. **Evidence of legal authority.** The Acquirer must provide:
   - a copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority, that expressly authorizes the Merchant to conduct the particular type of skill game(s) for which it wishes to accept Cards as payment for entry fees; and
   - any law applicable to the Merchant that permits the conduct of skill games.
2. **Legal opinion.** The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a private sector U.S. lawyer or U.S. law firm. The legal opinion must:
   - identify all relevant laws that address the conduct of skill games (e.g., anti-gambling laws that provide an exemption for skill games) and other laws applicable to the Merchant's skill games activities;
   - identify all relevant laws that address the participation in skill games and other laws applicable to Cardholders permitted by the Merchant to participate in skill games with the Merchant; and
   - demonstrate that the Merchant's and Cardholders' skill games and payment activities comply at all times with any laws identified above.

   The Acquirer must provide Mastercard with a copy of such legal opinion. The legal opinion must be acceptable to Mastercard.
3. **Effective controls.** The Acquirer must provide certification from a qualified independent third party demonstrating that the Merchant's systems for operating its skill games business:
   - include effective age and location verification, as applicable; and
   - are reasonably designed to ensure that the Merchant's skill games business will remain within legal limits (including in connection with interstate Transactions).

   The certification must include all screenshots relevant to the certification (for example, age verification process). Certifications from interested parties (such as the Acquirer, ISOs, the Merchant, and so on) are not acceptable substitutes for the independent third-party certification.
4. **Notification of changes.** The Acquirer must certify that it will notify Mastercard of any changes to the information that it has provided to Mastercard, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to Mastercard (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.

5. **Acceptance of responsibilities.** The Acquirer must specifically affirm that it will not submit Restricted Transactions (as defined in the *Internet Gambling Policy*) from the Merchant for authorization.

Mastercard must approve the registration request before the Acquirer may process any skill games Transactions for the Merchant, Sponsored Merchant, or other entity.

9.4.6 High-Risk Cyberlocker Merchants

A non–face-to-face cyberlocker Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase access directly from a Merchant or Sponsored Merchant, or indirectly from an operator or entity that can provide access, to remote digital file storage and sharing services.

Before an Acquirer may process non–face-to-face cyberlocker Transactions from a Merchant or Sponsored Merchant whose contents and services meet one or more of the following criteria, it must register the Merchant or Sponsored Merchant, as well as any entities that can provide access to or accept payments on behalf of such Merchant's or Sponsored Merchant's contents and services, with Mastercard as described in section 9.2 of this manual:

- The cyberlocker Merchant provides rewards, cash payments, or other incentives to uploaders. Some incentives are based on the number of times that the uploader's files are downloaded or streamed by third parties. The Merchant's rewards programs also pay a higher commission for the distribution of file sizes consistent with long-form copyrighted content such as movies and television shows.
- The cyberlocker Merchant provides URL codes to uploaders to facilitate sharing and the incorporation of such links on third-party indexing or linking websites.
- Links to prohibited content stored in the cyberlocker are often found on third-party indexing or linking sites, or by search engine queries.
- Files stored within the cyberlocker Merchant may be purged if they are not accessed or unless the user purchases a premium membership.
- Incentives for premium cyberlocker memberships are based on faster download speed or removing ads, as opposed to storage space. Free access to stored files may otherwise be discouraged by long wait times, bandwidth throttling, download limits, online advertising, or other techniques.
- The cyberlocker Merchant provides a "link checker" that allows users to determine whether a link has been removed, and if so, allows the user to promptly re-upload that content.
- File owners are:
  - Typically anonymous,
  - Not required to provide any identifying information, and
  - Not aware of the identity of those users who have access to or view their files.
- File distribution and sharing are emphasized on the cyberlocker site.
- Storage or transfer of specific copyrighted file types such as movies, videos, or music is promoted on the cyberlocker site.
- Without the purchase of a premium membership, video playback includes frequent display advertisements.

An Acquirer must identify all non–face-to-face cyberlocker Transactions using MCC 4816 (Computer Network/Information Services) and TCC T.

At the time of registration of a Merchant, Sponsored Merchant, or entity in accordance with this section, the Acquirer of such Merchant, Sponsored Merchant, or entity must have verified that the Merchant's, Sponsored Merchant's, or entity's activity complies fully with all laws applicable to Mastercard, the Merchant, Sponsored Merchant, entity, the Issuer, the Acquirer, and any prospective customer of the Merchant, Sponsored Merchant, or entity. Such verification may include, but is not limited to, a written opinion from independent, reputable, and qualified legal counsel or accreditation by a recognized third party.

By registering a Merchant, Sponsored Merchant, or entity as required by this section, the Acquirer represents and warrants that the Acquirer has verified compliance with applicable law as described above. The Acquirer must maintain such verification for so long as it acquires Transactions from the Merchant, Sponsored Merchant, or entity that is subject to the aforedescribed registration requirement and must, no less frequently than every 12 months, confirm continued compliance with applicable law concerning the business of the registered Merchant, Sponsored Merchant, or entity. The Acquirer must furnish Mastercard with a copy of such documentation promptly upon request.

9.4.7 Recreational Cannabis Merchants (Canada Region Only)

Before acquiring Transactions reflecting the purchase of recreational cannabis at a Merchant or Sponsored Merchant located in the Canada Region, an Acquirer first must register the Merchant or Sponsored Merchant with Mastercard as described in section 9.2 and this section 9.4.7.

A Canada Region Acquirer must:

- Use MCC 5912 (Drug Stores, Pharmacies) to identify Transactions arising from a Canada Region Merchant or Sponsored Merchant whose primary business is the sale of recreational cannabis (For a Canada Region Merchant or Sponsored Merchant whose primary business is not the sale of recreational cannabis, the MCC of the Merchant's or Sponsored Merchant's primary business must be used); and
- Obtain and retain from the Merchant or Sponsored Merchant or a Canadian provincial licensing authority a copy of the provincial retail license permitting the Merchant or Sponsored Merchant to sell cannabis for recreational purposes. The Acquirer must furnish Mastercard with a copy of such documentation promptly upon request.
- Notify Mastercard in writing of any change to the information that the Acquirer provided to Mastercard as part of the registration process, including any change in the Merchant's or Sponsored Merchant's provincial retail license. Such notification is required within ten (10) business days of any such change.

In the event that a recreational cannabis Merchant or Sponsored Merchant loses its licensed status, the Acquirer must stop the Merchant or Sponsored Merchant from accepting Mastercard-branded payments products for recreational cannabis sales and promptly advise Mastercard in writing of such action.

9.4.8 High-Risk Securities Merchants

A securities Transaction occurs directly or indirectly in a Card-present or Card-not-present environment when a consumer uses an Account to purchase, sell, or broker a financial instrument, including but not limited to derivatives (for example: forwards, futures, options, and swaps).

Before an Acquirer may process securities Transactions from a Merchant, Sponsored Merchant, or other entity that facilitates one or more of the following activities, the Acquirer must register the Merchant, Sponsored Merchant, or other entity with Mastercard as described in section 9.2 of this manual.

- Binary options trading
- Contracts for difference (CFD)
- Foreign exchange (Forex) currency options trading
- Cryptocurrency options trading
- Initial coin offerings (ICOs)

An Acquirer must identify all high-risk securities Transactions using MCC 6211 (Securities—Brokers/Dealers) and TCC R (for face-to-face Transactions) or TCC T (for non-face-to-face Transactions), and a Transaction Type Identifier (TTI) value of P71 (High-risk Securities).

To register a Merchant, Sponsored Merchant, or other entity, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items to Mastercard upon request as part of the registration process (herein, all references to a Merchant also apply to a Sponsored Merchant or other entity):

1. **Evidence of legal authority**. The Acquirer must obtain from the Merchant:
   - a copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority in each country where high-risk trading activity as described in this section will occur or be offered to Cardholders, that expressly authorizes the Merchant to engage in such trading activity;
   - a copy of the Merchant's registration, where required under applicable law, with a licensed exchange or licensed trading platform; and
   - any law applicable to the Merchant that permits such high-risk trading activity.

   The Acquirer must provide an updated license(s) to Mastercard prior to expiration. If an Acquirer is unable to obtain an updated license, then the Acquirer must cease processing applicable high-risk securities Transactions from such Merchant until the Acquirer is able to provide an updated license to Mastercard.
2. **Legal opinion.** The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a reputable law firm located in each country where high-risk trading activity as described in this section will occur or be offered to Cardholders. The legal opinion must:
   - identify all relevant trading laws and other laws applicable to the Merchant;
   - identify all relevant trading laws and other laws applicable to Cardholders that may transact with the Merchant; and
   - demonstrate that the Merchant's and Cardholders' trading activities comply at all times with any laws identified above.

The legal opinion must be acceptable to Mastercard. Further, the Acquirer shall ensure that:

- the Merchant properly maintains its lawful status in any jurisdiction where such Merchant engages in high-risk trading activities as described in this section; and
- any relevant permits remain unexpired.

3. **Effective controls.** The Acquirer must obtain certification from a qualified independent third party demonstrating that the Merchant's systems for operating its high-risk securities business:
   - include effective age and location verification; and
   - are reasonably designed to ensure that the Merchant's high-risk securities business will remain within legal limits (including in connection with cross-border Transactions).
4. **Notification of changes.** The Acquirer must certify that the Acquirer will notify Mastercard of any changes to the information that the Acquirer has provided to Mastercard, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to Mastercard (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.
5. **Acceptance of responsibilities.** The Acquirer must specifically affirm that it will not submit restricted Transactions from the Merchant for authorization.

If a Merchant's non-face-to-face high-risk trading activities are regulated as gambling in any jurisdiction, then the Acquirer must register such Merchant as a non-face-to-face gambling Merchant with Mastercard as described in section 9.2 and section 9.4.2 of this manual.

9.4.9 Cryptocurrency Merchants

A cryptocurrency Transaction occurs in a Card-present or Card-not-present environment when a consumer uses an Account to:

- Directly purchase a digital asset recognized as a medium of exchange, unit of account, and store of value that uses cryptography to secure Transactions associated with the digital asset, control the generation of additional cryptocurrency units, and verify the transfer of funds;
  Or
- Purchase, sell, or trade such a digital asset by means of a digital currency, alternative currency, or virtual currency exchange platform.

The recognition of a cryptocurrency as a medium of exchange, unit of account, and store of value occurs only by agreement within the community of users of such cryptocurrency. For the avoidance of doubt, legal tender or virtual currency issued by a government or centralized banking system is not considered cryptocurrency.

Before an Acquirer may process cryptocurrency Transactions from a Merchant, Sponsored Merchant, or other entity, the Acquirer must register the Merchant, Sponsored Merchant, or other entity with Mastercard as described in section 9.2 of this manual and obtain from the Merchant, Sponsored Merchant, or other entity:

- a copy of the license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority in each country where cryptocurrency activity will

occur or be offered to Cardholders, that expressly authorizes the entity to engage in such activity; and

- a copy of the entity's registration, where required under applicable law, with a licensed exchange or licensed trading platform.

An Acquirer must identify all cryptocurrency Transactions using MCC 6051 (Quasi Cash—Merchant), TCC U, and a Transaction Type Identifier (TTI) value of P70 (Cryptocurrency), in each Transaction.

At the time of registration of a Merchant, Sponsored Merchant, or other entity in accordance with this section, the Acquirer of such entity must have verified that the entity's activity complies fully with all laws and regulations applicable to Mastercard, the entity, the Issuer, the Acquirer, and any prospective customer of the entity. Such verification may include, but is not limited to, a written opinion from independent, reputable, and qualified legal counsel or accreditation by a recognized third party.

By registering a Merchant, Sponsored Merchant, or other entity as required by this section, the Acquirer represents and warrants that the Acquirer has verified compliance with applicable law as described above. The Acquirer must maintain such verification for so long as it acquires Transactions from the Merchant, Sponsored Merchant, or other entity that is subject to the aforedescribed registration requirement and must, no less frequently than every 12 months or if any applicable laws and regulations change, confirm continued compliance with applicable law concerning the business of the registered Merchant, Sponsored Merchant, or other entity. The Acquirer must furnish Mastercard with a copy of such documentation promptly upon request.

9.4.10 Negative Option Billing Merchants Selling Physical Products

A non-face-to-face negative option billing Transaction for the sale of physical products occurs in a Card-not-present environment when a consumer uses an Account to purchase a subscription service to automatically receive one or more physical products (such as cosmetics, health-care products, or vitamins) on a recurring basis (such as weekly, monthly, semi-annually, or annually).

The subscription service may be initiated by an agreement between the consumer and the Merchant or Sponsored Merchant whereby the consumer (Cardholder) receives from the Merchant or Sponsored Merchant a sample of the product (either complimentary or at a nominal price) for a trial period. The sample may be larger, equal to, or smaller than the product provided by the Merchant or Sponsored Merchant during the subscription period. For the purposes of this section 9.4.10, a trial period means a preset length of time during which the Cardholder may evaluate the characteristics of the physical product such as its quality or usefulness to determine whether the Cardholder wants to either:

- Purchase the product on a one-time basis or recurring basis; or
- Return the product (if possible) to the negative option billing Merchant.

After the trial period has expired, a non-face-to-face negative option billing Transaction may occur upon the Cardholder's initiation of the subscription.

The non-face-to-face negative option billing Transactions continue to occur on a recurring basis until either:

- The Cardholder takes action to terminate the agreement with the Merchant or Sponsored Merchant (for example, notifying the Merchant or Sponsored Merchant to cancel the subscription);
- The Merchant or Sponsored Merchant terminates the agreement; or
- The subscription expires.

Before an Acquirer may process non-face-to-face high-risk negative option billing Transactions involving physical products, including magazine and newspaper subscriptions, from a Merchant or Sponsored Merchant, the Acquirer must register the Merchant or Sponsored Merchant, as well as any entities that provide service to such Merchant or Sponsored Merchant that allow access to Account data, with Mastercard as described in section 9.2 of this manual.

An Acquirer must use MCC 5968 (Direct Marketing-Continuity/Subscription Merchants) and TCC T to identify all non-face-to-face negative option billing Transactions.

At the time of registration of a Merchant, Sponsored Merchant, or entity in accordance with this section 9.4.10, the Acquirer of such Merchant, Sponsored Merchant, or entity must have verified that the Merchant's, Sponsored Merchant's, or entity's activity complies fully with all laws applicable to Mastercard, the Merchant, Sponsored Merchant, entity, the Issuer, the Acquirer, and any prospective customer of the Merchant, Sponsored Merchant, or entity.

Chapter 10 Account Data Compromise Events

This chapter may be of particular interest to Customers that have experienced or wish to protect themselves against Account data compromise events.

10.1 Applicability and Defined Terms

NOTE: This chapter applies to Mastercard and Maestro Transactions, unless otherwise indicated.

Definitions

As used in this chapter, the following terms shall have the meaning set forth below:

Account Data Compromise Event or ADC Event

An occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of Account data or the unauthorized manipulation of Account data controls, such as Account usage and spending limits.

Agent

Any entity that stores, processes, transmits, or has access to Account data by virtue of its contractual or other relationship, direct or indirect, with a Customer. For the avoidance of doubt, Agents include, but are not limited to, Merchants, Third Party Processors (TPPs), Data Storage Entities (DSEs), AML/Sanctions Service Providers and Terminal Servicers (TSs) (regardless of whether the TPP, DSE, AML/Sanctions Service Providers or TS is registered with Mastercard).

Customer

This term appears in the Definitions appendix at the end of this manual. For the avoidance of doubt, for purposes of this chapter, any entity that Mastercard licenses to issue a Mastercard and/or Maestro Card(s) and/or acquire a Mastercard and/or Maestro Transaction(s) shall be deemed a Customer.

Digital Activity Customer

This term appears in the Definitions appendix at the end of this manual. For the avoidance of doubt, for purposes of this chapter, any entity that Mastercard has approved to be a Wallet Token Requestor shall be deemed a Digital Activity Customer. A Digital Activity Customer is a type of Customer.

Hybrid Point-of-Sale (POS) Terminal

A terminal that (i) is capable of processing both Chip Transactions and magnetic stripe Transactions; and (ii) 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 (iii) has satisfactorily completed the Mastercard Terminal Integration Process (TIP) in the appropriate environment of use.

Potential Account Data Compromise Event or Potential ADC Event

An occurrence that could result, directly or indirectly, in the unauthorized access to or disclosure of Account data or the unauthorized manipulation of Account data controls, such as Account usage and spending limits.

Sensitive Authentication Data

This term has the meaning set forth in the *Payment Card Industry Data Security Standard* (PCI DSS), and includes, by way of example and not limitation, the full contents of a Card's magnetic stripe or the equivalent on a chip, Card validation code 2 (CVC 2) data, and PIN or PIN block data.

Standards

This term appears in the Definitions appendix at the end of this manual.

Wallet Token Requestor

This term appears in the Definitions appendix at the end of this manual.

Terms used in this chapter (such as Issuer, Acquirer, and Card) are used consistent with the definitions of such terms set forth in the Definitions appendix at the end of this manual. With regard to Accounts and Card issuance, Mastercard Standards reflect the use of different types of licensing structures and relationships, including:

- Principal Customer and Affiliate Customer;
- Association Customer and Affiliate Customer;
- Principal Debit Licensee and Affiliate Debit Licensee; and
- Type I TPP and Affiliate Customer (in the U.S. Region only).

For purposes of this chapter, an Issuer is the entity having responsibility in accordance with the Standards and, if applicable, any license agreement between the entity and Mastercard, with respect to Activity pertaining to a particular Card or Account.

10.2 Policy Concerning Account Data Compromise Events and Potential Account Data Compromise Events

Mastercard operates a payment solutions system for all of its Customers. Each Customer benefits from, and depends upon, the integrity of that system. ADC Events and Potential ADC Events threaten the integrity of the Mastercard system and undermine the confidence of Merchants, Customers, Cardholders, and the public at large in the security and viability of the system. Each Customer therefore acknowledges that Mastercard has a compelling interest in adopting, interpreting, and enforcing its Standards to protect against and respond to ADC Events and Potential ADC Events.

Given the abundance and sophistication of criminals, ADC Events and Potential ADC Events are risks inherent in operating and participating in any system that utilizes payment card account data for financial or non-financial transactions. Mastercard Standards are designed to place responsibility for ADC Events and Potential ADC Events on the Customer that is in the best position to guard against and respond to such risk. That Customer is generally the Customer whose network, system, or environment was compromised or was vulnerable to compromise or that has a direct or indirect relationship with an Agent whose network, system, or environment was compromised or was vulnerable to compromise. In the view of Mastercard, that Customer

is in the best position to safeguard its systems, to require and monitor the safeguarding of its Agents' systems, and to insure against, and respond to, ADC Events and Potential ADC Events.

Mastercard requires that each Customer apply the utmost diligence and forthrightness in protecting against and responding to any ADC Event or Potential ADC Event. Each Customer acknowledges and agrees that Mastercard has both the right and need to obtain full disclosure (as determined by Mastercard) concerning the causes and effects of an ADC Event or Potential ADC Event as well as the authority to impose assessments, recover costs, and administer compensation, if appropriate, to Customers that have incurred costs, expenses, losses, and/or other liabilities in connection with ADC Events and Potential ADC Events.

Except as otherwise expressly provided for in the Standards, Mastercard determinations with respect to the occurrence of and responsibility for ADC Events or Potential ADC Events are conclusive and are not subject to appeal or review within Mastercard.

Any Customer that is uncertain with respect to rights and obligations relating to or arising in connection with the Account Data Compromise Event Standards and Programs set forth in this Chapter 10 should request advice from Mastercard.

Notwithstanding the generality of the foregoing, the relationship of network, system, and environment configurations with other networks, systems, and environments will often vary, and each ADC Event and Potential ADC Event tends to have its own particular set of circumstances. Mastercard has the sole authority to interpret and enforce the Standards, including those set forth in this chapter. Consistent with the foregoing and pursuant to the definitions set forth in section 10.1 above, Mastercard may determine, as a threshold matter, whether a given set of circumstances constitutes a single ADC Event or multiple ADC Events. In this regard, and by way of example, where a Customer or Merchant connects to, utilizes, accesses, or participates in a common network, system, or environment with one or more other Customers, Merchants, Service Providers, or third parties, a breach of the common network, system, or environment that results, directly or indirectly, in the compromise of local networks, systems, or environments connected thereto may be deemed to constitute a single ADC Event.

10.3 Responsibilities in Connection with ADC Events and Potential ADC Events

The Customer whose system or environment, or whose Agent's system or environment, was compromised or vulnerable to compromise (at the time that the ADC Event or Potential ADC Event occurred) is fully responsible for resolving all outstanding issues and liabilities to the satisfaction of Mastercard, notwithstanding any subsequent change in the Customer's relationship with any such Agent after the ADC Event or Potential ADC Event occurred. In the event of any dispute, Mastercard will determine the responsible Customer(s).

Should a Customer, in the judgment of Mastercard, fail to fully cooperate with the Mastercard investigation of an ADC Event or Potential ADC Event, Mastercard (i) may infer that information sought by Mastercard, but not obtained as a result of the failure to cooperate, would be unfavorable to that Customer and (ii) may act upon that adverse inference in the application of the Standards. By way of example and not limitation, a failure to cooperate can

result from a failure to provide requested information; a failure to cooperate with Mastercard investigation guidelines, procedures, practices, and the like; or a failure to ensure that Mastercard has reasonably unfettered access to the forensic examiner.

A Customer may not, by refusing to cooperate with the Mastercard investigation, avoid a determination that there was an ADC Event. Should a Customer fail without good cause to comply with its obligations in this Chapter 10 or to respond fully and in a timely fashion to a request for information to which Mastercard is entitled in this Chapter 10, Mastercard may draw an adverse inference that information to which Mastercard is entitled, but that was not timely obtained as a result of the Customer's noncompliance, would have supported or, where appropriate, confirmed a determination that there was an ADC Event.

Before drawing such an adverse inference, Mastercard will notify the Customer of its noncompliance and give the Customer an opportunity to show good cause, if any, for its noncompliance. The drawing of an adverse inference is not exclusive of other remedies that may be invoked for a Customer's noncompliance.

The following provisions set forth requirements and procedures to which each Customer and its Agent(s) must adhere upon becoming aware of an ADC Event or Potential ADC Event.

10.3.1 Time-Specific Procedures for ADC Events and Potential ADC Events

A Customer is deemed to be aware of an ADC Event or Potential ADC Event when the Customer or the Customer's Agent first knew or, in the exercise of reasonable security practices should have known of an ADC Event or a Potential ADC Event. A Customer or its Agent is deemed to be aware of an ADC Event or Potential ADC Event under circumstances that include, but are not limited to, any of the following:

- the Customer or its Agent is informed, through any source, of the installation or existence of any malware in any of its systems or environments, or any system or environment of one of its Agents, no matter where such malware is located or how it was introduced;
- the Customer or its Agent receives notification from Mastercard or any other source that the Customer or its Agent(s) has experienced an ADC Event or a Potential ADC Event; or
- the Customer or its Agent discovers or, in the exercise of reasonable diligence, should have discovered a security breach or unauthorized penetration of its own system or environment or the system or environment of its Agent(s).

A Customer must notify Mastercard immediately when the Customer becomes aware of an ADC Event or Potential ADC Event in or affecting any system or environment of the Customer or its Agent. In addition, a Customer must, by contract, ensure that its Agent notifies Mastercard immediately when the Agent becomes aware of an ADC Event or Potential ADC Event in or affecting any system or environment of the Customer or the Agent.

When a Customer or its Agent becomes aware of an ADC Event or Potential ADC Event either in any of its own systems or environments or in the systems or environments of its Agent(s), the Customer must take (or cause the Agent to take) the following actions, unless otherwise directed in writing by Mastercard.

- Immediately notify Mastercard of the ADC Event or Potential ADC Event.
- Immediately commence a thorough investigation into the ADC Event or Potential ADC Event.

- Immediately, and no later than within twenty-four (24) hours, identify, contain, and mitigate the ADC Event or Potential ADC Event, secure Account data and preserve all information, in all media, concerning the ADC Event or Potential ADC Event, including:
  1. preserve and safeguard all potential evidence pertinent to a forensic examination of an ADC Event or Potential ADC Event using industry best practices;
  2. isolate compromised systems and media from the network using industry best practices;
  3. preserve all Intrusion Detection Systems, Intrusion Prevention System logs, all firewall, Web, database, and events logs;
  4. document all incident response actions thoroughly; and
  5. refrain from restarting or rebooting any compromised or potentially compromised system or taking equivalent or other action that would have the effect of eliminating or destroying information that could potentially provide evidence of an ADC Event or Potential ADC Event.
- Within twenty-four (24) hours, and on an ongoing basis thereafter, submit to Mastercard all known or suspected facts concerning the ADC Event or Potential ADC Event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the ADC Event or Potential ADC Event to the satisfaction of Mastercard.
- Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to Mastercard, in the required format, all primary account numbers (PANs) associated with Account data that were actually or potentially accessed or disclosed in connection with the ADC Event or Potential ADC Event and any additional information requested by Mastercard. As used herein, the obligation to obtain and provide PANs to Mastercard applies to any Mastercard or Maestro Account number in a bank identification number (BIN)/Issuer identification number (IIN) range assigned by Mastercard. This obligation applies regardless of how or why such PANs were received, processed, or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature- or PIN-based) proprietary, or any other kind of payment Transaction, incentive, or reward program.
- Within seventy-two (72) hours, engage the services of a Payment Card Industry Security Standards Council (PCI SSC) Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC Event or Potential ADC Event. The PFI engaged to conduct the investigation must remain free of conflict of interest as defined in the *PFI Program Guide*. Prior to the commencement of such PFI's investigation, the Customer must notify Mastercard of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by Mastercard or, if such preliminary approval is not obtained, of a modified proposal acceptable to Mastercard. Mastercard and the responsible Customer(s) may agree that a PFI's investigation of, investigation findings, and recommendations concerning fewer than all of the Merchants (or other Agents) within the scope of the ADC Event or Potential ADC Event will be deemed to be representative of and used for purposes of the application of the Standards as the investigation findings and recommendations by the PFI with respect to all of the Merchants (or other Agents) within the scope of the ADC Event or Potential ADC Event.
- Within two (2) business days from the date on which the PFI was engaged, identify to Mastercard the engaged PFI and confirm that such PFI has commenced its investigation.

- Within five (5) business days from the commencement of the forensic investigation, ensure that the PFI submits to Mastercard a preliminary forensic report detailing all investigative findings to date.
- Within ten (10) business days from the end of the PFI investigation, provide to Mastercard a final forensic report detailing all findings, conclusions, and recommendations of the PFI, continue to address any outstanding exposure, and implement all recommendations until the ADC Event or Potential ADC Event is resolved to the satisfaction of Mastercard. In connection with the independent forensic investigation and preparation of the final forensic report, no Customer may engage in or enter into (or permit an Agent to engage in or enter into) any conduct, agreement, or understanding that would impair the completeness, accuracy, or objectivity of any aspect of the forensic investigation or final forensic report. The Customer shall not engage in any conduct (or permit an Agent to engage in any conduct) that could or would influence, or undermine the independence of, the PFI or undermine the reliability or integrity of the forensic investigation or final forensic report. By way of example, and not limitation, a Customer must not itself, or permit any of its Agents to, take any action or fail to take any action that would have the effect of:
  1. precluding, prohibiting, or inhibiting the PFI from communicating directly with Mastercard;
  2. permitting a Customer or its Agent to substantively edit or otherwise alter the forensic report; or
  3. directing the PFI to withhold information from Mastercard.

Notwithstanding the foregoing, Mastercard may engage a PFI on behalf of the Customer in order to expedite the investigation. The Customer on whose behalf the PFI is so engaged will be responsible for all costs associated with the investigation.

10.3.2 Ongoing Procedures for ADC Events and Potential ADC Events

From the time that the Customer or its Agent becomes aware of an ADC Event or Potential ADC Event until the investigation is concluded to the satisfaction of Mastercard, the Customer must:

- Provide weekly written status reports containing current, accurate, and updated information concerning the ADC Event or Potential ADC Event, the steps being taken to investigate and remediate same, and such other information as Mastercard may request.
- Preserve all files, data, and other information pertinent to the ADC Event or Potential ADC Event, and refrain from taking any actions (e.g., rebooting) that could result in the alteration or loss of any such files, forensic data sources, including firewall and event log files, or other information.
- Respond fully and promptly, in the manner prescribed by Mastercard, to any questions or other requests (including follow-up requests) from Mastercard with regard to the ADC Event or Potential ADC Event and the steps being taken to investigate and remediate same.
- Authorize and require the PFI to respond fully, directly, and promptly to any written or oral questions or other requests from Mastercard, and to so respond in the manner prescribed by Mastercard, with regard to the ADC Event or Potential ADC Event, including the steps being taken to investigate and remediate same.

- Consent to, and cooperate with, any effort by Mastercard to engage and direct a PFI to perform an investigation and prepare a forensic report concerning the ADC Event or Potential ADC Event, in the event that the Customer fails to satisfy any of the foregoing responsibilities.
- Ensure that the compromised entity develops a remediation action plan, including implementation and milestone dates related to findings, corrective measures, and recommendations identified by the PFI and set forth in the final forensic report.
- Monitor and validate that the compromised entity has fully implemented the remediation action plan, recommendations, and corrective measures.

10.4 Forensic Report

The responsible Customer (or its Agent) must ensure that the PFI retains and safeguards all draft forensic report(s) pertaining to the ADC Event or Potential ADC Event and, upon request of Mastercard, immediately provides to Mastercard any such draft. The PFI should adhere to the PFI Program Guide as it pertains to the work products produced by the PFI.

Mastercard may require the Customer to cause a PFI to conduct a PCI gap analysis and include the result of that analysis in the final forensic report.

The Customer must direct the PFI to submit a copy of the preliminary and final forensic reports to Mastercard immediately upon completion.

10.5 Alternative Acquirer Investigation Standards

In the event of an ADC Event or Potential ADC Event (for purposes of this section 10.5, an "Event") for which the subject is a Level 2, Level 3, or Level 4 Merchant (as set forth in section 2.2.2), in lieu of complying with the responsible Customer obligations set forth in section 10.3.1, the first bullet point of section 10.3.2, and section 10.4 of this Chapter 10, a responsible Customer may comply with the Standards set forth in this section 10.5 provided all of the following criteria are satisfied:

Criterion A

Mastercard determines that fewer than 30,000 Accounts are potentially at risk of unauthorized disclosure as a result of the Event; and

Criterion B

Mastercard determines that the Merchant (or other Agent) has not been the subject of an ADC Event or Potential ADC Event for the thirty-six (36) consecutive months immediately preceding the date that Mastercard determines likely to be the earliest possible date of the Event; and

Criterion C

The responsible Customer determines that the Merchant (or other Agent) uses a payment acceptance system that does not share connectivity with another Merchant (or Agent) or Merchant's (or Agent's) system and that is not operated by a Service Provider.

Should Mastercard determine that the subject of the Event is a Level 2, 3, or 4 Merchant and that Criteria A and B, above, are satisfied, Mastercard will provide notice to the responsible Customer by way of an email message to the responsible Customer's Security Contact listed in the My Company Manager application then available on Mastercard Connect™.

Upon receipt of such notice, the responsible Customer may elect to cause a PFI to conduct an examination of the Merchant or other Agent in accordance with section 10.3.1 of this Chapter 10. Should the responsible Customer cause a PFI to conduct an examination, the responsible Customer must notify Mastercard within 24 hours of the engagement of the PFI. Failure to notify Mastercard within the 24-hour time frame may result in a noncompliance assessment as described in section 10.7. Alternatively, and provided the responsible Customer determines that Criterion C is satisfied, the responsible Customer itself may elect to investigate the Event in lieu of causing a PFI to conduct an examination of the Merchant or other Agent.

If the responsible Customer itself elects to conduct the investigation, not later than twenty (20) business days following the date of the notice by Mastercard described above, the responsible Customer must provide to Mastercard that all of the following are true:

- The responsible Customer elected to investigate the ADC Event or Potential ADC Event in lieu of causing a PFI to investigate the ADC Event or Potential ADC Event; and
- The Merchant (or other Agent) that is the subject of the ADC Event or Potential ADC Event does not use a computer-based acceptance system that is used by another Merchant (or Agent) or is connected to Merchants (or Agents) or third parties; and
- The responsible Customer's investigation of the ADC Event or Potential ADC Event has been completed and the ADC Event or Potential ADC Event has been fully contained. Documentation satisfactory to Mastercard confirming such containment (including the date of containment) and a written explanation of how the security event was contained (including the steps taken to ensure that Account data are no longer at risk of compromise) must be provided to Mastercard; and
- The Merchant has newly validated, or revalidated or has a road map to achieve compliance with the PCI DSS. Documentation confirming such validation or revalidation must be provided to Mastercard upon completion of the investigation.

Failure to comply with any obligation of the responsible Customer may result in the imposition of a noncompliance assessment as described in section 10.7.

Mastercard may conduct periodic reviews of an ADC Event or Potential ADC Event investigated by the responsible Customer to confirm that the Event has been fully contained. Should Mastercard determine that an Event continues to place Accounts at risk of unauthorized disclosure, Mastercard will provide notice to the responsible Customer by way of an email message to the responsible Customer's Security Contact then listed in the My Company Manager application.

Within ten (10) business days of such notice, the responsible Customer must provide to Mastercard a remediation action plan describing the steps (and relevant dates of the steps)

that the responsible Customer will take to ensure that Account data are no longer at risk of compromise. Failure to provide Mastercard with the remediation action plan within the 10-day time frame may result in a noncompliance assessment as described in section 10.7.

Within twenty (20) business days after Mastercard provides approval of the responsible Customer's remediation action plan, the responsible Customer must implement all required steps of the action plan, including but not limited to officer certification to Mastercard that such remediation action plan has taken effect. Failure to implement the remediation action plan to the satisfaction of Mastercard within the 20-day time frame may result in a noncompliance assessment as described in section 10.7.

If the Merchant (or Agent) that was the subject of an ADC Event or Potential ADC Event investigated by the responsible Customer is the subject of a different Event within thirty-six (36) months of the date on which Mastercard provided notice to the responsible Customer of the initial Event, Mastercard:

- Will require the responsible Customer to engage the services of a PFI to conduct an independent examination of the Merchant or other Agent in accordance with section 10.3.1 of this Chapter 10; and
- May impose an assessment of up to USD 25,000 upon the responsible Customer for failure to safeguard Account data.

Except as specifically set forth in this section 10.5, all other Mastercard and Customer rights and obligations with respect to an ADC Event or Potential ADC Event shall continue with respect to any ADC Event or Potential ADC Event that a responsible Customer itself elects to investigate in accordance with this section 10.5. Further, and for the avoidance of doubt, Mastercard has a right at any time to require a responsible Customer to cause a PFI to conduct a forensic examination of a Merchant notwithstanding the provisions of this section 10.5.

10.6 Mastercard Determination of ADC Event or Potential ADC Event

Mastercard will evaluate the totality of known circumstances, including but not limited to the following, to determine whether or not an occurrence constitutes an ADC Event or Potential ADC Event:

- a Customer or its Agent acknowledges or confirms the occurrence of an ADC Event or Potential ADC Event;
- any PFI report; or
- any information determined by Mastercard to be sufficiently reliable at the time of receipt.

10.6.1 Assessments for PCI Violations in Connection with ADC Events

Based on the totality of known circumstances surrounding an ADC Event or Potential ADC Event, including the knowledge and intent of the responsible Customer, Mastercard (in addition to any assessments provided for elsewhere in the Standards) may assess a responsible Customer up to USD 100,000 for each violation of a requirement of the PCI SSC.

10.6.2 Potential Reduction of Financial Responsibility

Notwithstanding a Mastercard determination that an ADC Event occurred, Mastercard may consider any actions taken by the compromised entity to establish, implement, and maintain procedures and support best practices to safeguard Account data prior to, during, and after the ADC Event or Potential ADC Event, in order to relieve, partially or fully, an otherwise responsible Customer of responsibility for any assessments, ADC operational reimbursement, and/or investigative costs. In determining whether to relieve a responsible Customer of any or all financial responsibility, Mastercard may consider whether the Customer has complied with all of the following requirements:

- Substantiation to Mastercard from a PCI SSC-approved Qualified Security Assessor (QSA) of the compromised entity's compliance with the PCI DSS at the time of the ADC Event or Potential ADC Event.
- Reporting that certifies any Merchant(s) associated with the ADC Event or Potential ADC Event as compliant with the PCI DSS and all applicable Mastercard Site Data Protection (SDP) Program requirements at the time of the ADC Event or Potential ADC Event in accordance with section 2.2.1 of this manual. Such reporting must also affirm that all third party-provided payment applications used by the Merchant(s) associated with the ADC Event or Potential ADC Event are compliant with the *Payment Card Industry Payment Application Data Security Standard* or the *Payment Card Industry Secure Software Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide* and the applicability of the PCI Secure Software Standard to third party-provided payment software is defined in the *PCI Secure Software Program Guide*, found at www.pcisecuritystandards.org.
- If the compromised entity is a Europe Region Merchant, a PFI has validated that the Merchant was compliant with milestones one and two of the *PCI DSS Prioritized Approach* at the time of the ADC Event or Potential ADC Event.
- Registration of any TPP(s) or DSE(s) associated with the ADC Event through Mastercard Connect, in accordance with Chapter 7 of the *Mastercard Rules*.
- Notification of an ADC Event or Potential ADC Event to and cooperation with Mastercard and, as appropriate, law enforcement authorities.
- Verification that the PFI investigation was initiated within seventy-two (72) hours of the ADC Event or Potential ADC Event and completed as soon as practical.
- Timely receipt by Mastercard of the unedited (by other than the forensic examiner) forensic examination findings.
- Evidence that the ADC Event or Potential ADC Event was not foreseeable or preventable by commercially reasonable means and that, on a continuing basis, best security practices were applied.

In connection with its evaluation of the Customer's or its Agent's actions, Mastercard will consider, and may draw adverse inferences from, evidence that a Customer or its Agent(s) deleted or altered data.

As soon as practicable, Mastercard will contact the Customer's Security Contact, Principal Contact, or Account Data Compromise Contact as they are listed in the My Company Manager

application, notifying all impacted parties of the impending financial obligation or compensation, as applicable.

It is the sole responsibility of each Customer, not Mastercard, to include current and complete information in the My Company Manager application.

10.6.2.1 Potential Reduction of Financial Responsibility for Terminal Servicer ADC Events

Notwithstanding a Mastercard determination that an ADC Event occurred, Mastercard may consider the following actions taken by the compromised TS or the responsible Customer, as applicable, to establish, implement, and maintain procedures and support best practices to safeguard Account data prior to, during, and after the ADC Event or Potential ADC Event, in order to relieve, partially or fully, an otherwise responsible Customer of responsibility for any assessments, ADC operational reimbursement, and/or investigative costs. In determining whether to relieve a responsible Customer of any or all financial responsibility, Mastercard may consider whether the Terminal Servicer or the responsible Customer, as applicable, complied with all of the following requirements:

- Substantiation to Mastercard from a PCI SSC-approved QSA of the compromised TS's compliance with the PCI DSS at the time of the ADC Event or Potential ADC Event.
- Reporting that certifies any Terminal Servicer(s) associated with the ADC Event or Potential ADC Event as compliant with the PCI DSS and all applicable Mastercard SDP Program requirements at the time of the ADC Event or Potential ADC Event in accordance with section 2.2.3 of this manual. Such reporting must also affirm that all third party-provided payment applications used by the Terminal Servicer(s) associated with the ADC Event or Potential ADC Event are compliant with the *Payment Card Industry Payment Application Data Security Standard* or the *Payment Card Industry Secure Software Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide* and the applicability of the PCI Secure Software Standard to third party-provided payment software is defined in the *PCI Secure Software Program Guide*, found at www.pcisecuritystandards.org.
- Registration of any TS(s) associated with the ADC Event through Mastercard Connect, in accordance with Chapter 7 of the *Mastercard Rules*, within 10 calendar days of the TS or the responsible Customer being deemed aware of the ADC Event or Potential ADC Event.
- Notification of an ADC Event or Potential ADC Event to and cooperation with Mastercard and, as appropriate, law enforcement authorities.
- Verification that the PFI investigation was initiated within seventy-two (72) hours of the ADC Event or Potential ADC Event and completed as soon as practical.
- Timely receipt by Mastercard of the unedited (by other than the forensic examiner) forensic examination findings.
- Confirmation that any TS(s) associated with the ADC Event or Potential ADC Event completed all of the containment recommendations set forth in the forensic report, and that each such TS revalidated its compliance with the PCI DSS to Mastercard within 90 calendar days after the conclusion of the PFI's investigation and has additionally demonstrated compliance with the DESV appendix of the PCI DSS within twelve (12) months from achieving full compliance with the PCI DSS.

In connection with its evaluation of the Customer's or its TS's actions, Mastercard will consider, and may draw adverse inferences from, evidence that a Customer or its TS(s) deleted or altered data.

As soon as practicable, Mastercard will contact the Customer's Security Contact, Principal Contact, or Account Data Compromise Contact as they are listed in the My Company Manager application, notifying all impacted parties of the impending financial obligation or compensation, as applicable.

It is the sole responsibility of each Customer, not Mastercard, to include current and complete information in the Company Contact Management application.

10.6.3 ADC Operational Reimbursement—Mastercard Only

NOTE: This section applies to Mastercard Transactions only.

ADC operational reimbursement (OR) enables an Issuer to partially recover costs incurred in reissuing Cards and for enhanced monitoring of compromised and/or potentially compromised Mastercard Accounts associated with an ADC Event.

Mastercard may invoke OR for an ADC Event impacting 30,000 Mastercard Accounts or more. For purposes of this section 10.6.3, Mastercard generally deems an ADC Event to occur in the year in which Mastercard publishes an initial ADC Alert to impacted Issuers concerning the ADC Event. Mastercard reserves the right, however, to determine that an ADC Event occurred in a year other than the year in which Mastercard published an initial ADC Alert to impacted Issuers concerning the ADC Event.

Following the conclusion of an investigation, the OR, if any, will be disclosed to the responsible Customer(s) in a final financial liability letter. The responsible Customer(s) has 30 days following the date of the final financial liability letter to appeal the liability.

Partial operational reimbursement is available to an Issuer that is licensed to access the ADC application at the time of the ADC Event. Mastercard reserves the right to determine whether any ADC Event is eligible for ADC operational reimbursement and to limit or "claw back" ADC operational reimbursement based on the amount collected from the responsible Customer, excluding assessments, or for the purpose of compromising any claim asserted that arises from or is related to an ADC Event.

With regard to any particular ADC Event, Mastercard has no obligation to disburse an amount in excess of the amount that Mastercard actually and finally collects from the responsible Customer. In that regard, (i) any such amount actually and finally charged to a responsible Customer with respect to a particular ADC Event is determined by Mastercard following the full and final resolution of any claim asserted against Mastercard that arises from or is related to that ADC Event; and (ii) any funds disbursed by Mastercard to a Customer as ADC operational reimbursement is disbursed conditionally and subject to "claw back" until any claim and all claims asserted against Mastercard that arise from or are related to the ADC Event are fully and finally resolved.

In the administration of the ADC OR program, Mastercard may determine the responsible Customer's financial responsibility with respect to an ADC Event. When determining financial

responsibility, Mastercard may take into consideration the compromised entity's PCI level (as set forth in section 2.2.2 for Merchants and in section 2.2.3 for Service Providers), annual sales volume, and the factors set forth in section 10.6.2.

The annual sales volume is derived from the Merchant's clearing Transactions processed during the previous calendar year through the Global Clearing Management System (GCMS). Transactions that are not processed by Mastercard will be included in the annual sales volume if such data is available. In the event that the Merchant's annual sales volume is not known, Mastercard will use the Merchant's existing sales volume to project the annual sales volume or request said volume from the responsible Customer.

10.6.4 Determination of Operational Reimbursement (OR)

NOTE: This section applies to Mastercard Transactions only.

Subject to section 10.6.3, Mastercard generally determines OR in accordance with the following steps. Mastercard reserves the right to determine OR by an alternative means if Mastercard determines that information needed to use the following steps is not readily available. For additional information pertaining to OR, refer to the Mastercard *Account Data Compromise User Guide*.

1. Mastercard determines the number of at-risk Accounts per Issuer ICA number by type of Card. Accounts that have been disclosed in a previous ADC Alert in connection with a different ADC Event within 180 days prior to the publication of the ADC Alert for the ADC Event under review will be excluded from the calculation. Effective 31 December 2016, at-risk magnetic stripe-only Card Accounts (i.e., non-EMV chip Card Accounts) will be excluded from the calculation as well.
2. Mastercard multiplies the number of at-risk Accounts by an amount fixed by Mastercard from time to time.
3. From the results of Steps 1 and 2, Mastercard may subtract a fixed deductible (published in a Mastercard Announcement [AN] available on the Technical Resource Center on Mastercard Connect, or other Mastercard publication), to account for Card expirations and Card re-issuance cycles.
4. **United States Region Only**—For an ADC Event investigation opened by Mastercard on or after 1 October 2013, Mastercard will:

    a. Halve the amount determined by Steps 1, 2, and 3, above, if the compromised entity is a U.S. Region Acquirer's Merchant located in the U.S. Region and Mastercard determines that (i) at least seventy-five percent (75%) of the Merchant's annual total Transaction count was processed through Hybrid POS Terminals; and (ii) at least seventy-five percent (75%) of the Transactions deemed by Mastercard to be within the scope of the ADC Event were processed through Hybrid POS Terminals; and (iii) the Merchant has not been identified by Mastercard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest ADC Alert for the subject ADC Event; and (iv) Mastercard determines that the Merchant was not storing Sensitive Authentication Data; or

b. Effective 1 October 2015, not assess OR if the compromised entity is a U.S. Region Acquirer's Merchant located in the U.S. Region and Mastercard determines that (i) at least ninety-five percent (95%) of the Merchant's annual total Transaction count was acquired through Hybrid POS Terminals; and (ii) at least ninety-five percent (95%) of the Transactions deemed by Mastercard to be within the scope of the ADC Event were acquired through Hybrid POS Terminals; and (iii) the Merchant has not been identified by Mastercard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest ADC Alert for the subject ADC Event; and (iv) Mastercard determines that the Merchant was not storing Sensitive Authentication Data.

   For purposes of this Step 4, a Merchant's annual total Transaction count is determined based on the Merchant's clearing Transactions processed during the twelve (12) months prior to the date of publication of the ADC Alert through the GCMS. Transactions not processed by Mastercard are included in the annual Transaction count only if data pertaining to such Transactions is readily available to Mastercard. In the event that Mastercard is unable to readily determine the Merchant's actual annual total Transaction count, Mastercard may exercise its judgment to determine an annual total Transaction count. Mastercard may require an Acquirer to provide information to Mastercard for that purpose.

5. **United States Region Only**—For an ADC Event investigation opened by Mastercard on or after 1 October 2013, Mastercard will:
   a. Halve the amount determined by Steps 1, 2, and 3, above, if the compromised entity is a U.S. Region Acquirer's Merchant located in the U.S. Region and Mastercard determines that (i) at least seventy-five percent (75%) of the Merchant's annual total Transaction count was Tokenized using a Token Service Provider; and (ii) at least twenty-five percent (25%) of the Transactions deemed by Mastercard to be within the scope of the ADC Event were processed as e-commerce Transactions; and (iii) the Merchant has not been identified by Mastercard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest ADC Alert for the subject ADC Event; and (iv) Mastercard determines that the Merchant was not storing Sensitive Authentication Data; or
   b. Not assess OR if the compromised entity is a U.S. Region Acquirer's Merchant located in the U.S. Region and Mastercard determines that (i) at least ninety-five percent (95%) of the Merchant's annual total Transaction count was Tokenized using a Token Service Provider; and (ii) at least five percent (5%) of the Transactions deemed by Mastercard to be within the scope of the ADC Event were processed as e-commerce Transactions; and (iii) the Merchant has not been identified by Mastercard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest ADC Alert for the subject ADC Event; and (iv) Mastercard determines that the Merchant was not storing Sensitive Authentication Data.
6. **All Regions Other than the U.S. Region**—For an ADC Event investigation opened by Mastercard on or after 1 December 2014, Mastercard will determine OR in the manner set forth in Step 4, above, provided the requisite percentage of processed Transactions were processed through Hybrid POS Terminals.

10.6.5 Determination of Fraud Recovery (FR)

NOTE: This section applies to Mastercard Transactions only.

Mastercard determines FR in the manner set forth in this section.

Subject to section 10.6.3, Mastercard determines an amount of incremental counterfeit fraud attributable to an ADC Event based on the fraud data reported to the Fraud and Loss Database. As used in the immediately preceding sentence, the word "incremental counterfeit fraud" means counterfeit fraud incremental to the counterfeit fraud that Mastercard determines would have been expected to occur had the ADC Event not occurred. Effective 31 December 2016, at-risk Accounts issued on magnetic stripe-only Cards ("magnetic stripe-only Card Accounts") will be excluded from this determination and ineligible for FR. For additional information pertaining to FR, refer to the Mastercard *Account Data Compromise User Guide*.

NOTE: If the fraud type reported to the Fraud and Loss Database for one or more fraud Transactions is changed after Mastercard has calculated the ADC fraud recovery amount, Mastercard does not recalculate the ADC fraud recovery amount.

The calculation of FR uses an "at-risk time frame." The at-risk time frame may be known or unknown.

Known At-risk Time Frame

The at-risk time frame is "known" if Mastercard is able to determine a period of time during which Accounts were placed at risk of use in fraudulent Transactions due to or in connection with an ADC Event or Potential ADC Event. In such event, the at-risk time frame for an Account number commences as of the date that Mastercard determines that Account became at risk, and ends on the date specified in the first ADC Alert pertaining to that ADC Event or Potential ADC Event disclosing that Account number. The number of days that the Issuer has to report fraudulent Transactions to the Fraud and Loss Database associated with an Account number disclosed in an ADC Alert is specified in the Alert; an Issuer is ineligible to receive FR associated with a fraudulent Transaction arising from use of an Account number if that fraudulent Transaction is not timely reported to the Fraud and Loss Database. Mastercard will determine the number of days that the Issuer has to report fraudulent Transactions to the Fraud and Loss Database for a disclosed Account number as follows:

- If Mastercard publishes an ADC Alert before Mastercard has received a final PFI report concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 30, 45, or 60 days to report fraudulent Transactions to the Fraud and Loss Database.

NOTE: As set forth in Chapter 5 of the *ADC User's Guide*, Mastercard determines the number of days in which an Issuer must report fraudulent Transactions to the Fraud and Loss Database based on the number of Accounts placed at risk in the ADC Event or Potential ADC Event: (i) if an ADC Event or Potential ADC Event placed 30,000 to 1,000,000 Accounts at risk, then the number of days will be 30; (ii) if an ADC Event or Potential ADC Event placed 1,000,000 to 5,000,000 Accounts at risk, then the number of days will be 45; or (iii) if an ADC Event or Potential ADC Event placed at least 5,000,000 Accounts at risk, then the number of days will be 60.

- If Mastercard publishes an ADC Alert after Mastercard has received a final PFI report concerning the ADC Event or Potential ADC Event and a previous ADC Alert concerning the ADC Event has been published by Mastercard, then that ADC Alert will specify whether the Issuer has 20, 35, or 50 days to report fraudulent Transactions to the Fraud and Loss Database.

  NOTE: As set forth in Chapter 5 of the *ADC User's Guide*, Mastercard determines the number of days in which an Issuer must report fraudulent Transactions to the Fraud and Loss Database based on the number of Accounts placed at risk in the ADC Event or Potential ADC Event: (i) if an ADC Event or Potential ADC Event placed 30,000 to 1,000,000 Accounts at risk, then the number of days will be 20; (ii) if an ADC Event or Potential ADC Event placed 1,000,000 to 5,000,000 Accounts at risk, then the number of days will be 35; or (iii) if an ADC Event or Potential ADC Event placed at least 5,000,000 Accounts at risk, then the number of days will be 50.

Unknown At-risk Time Frame

The at-risk time frame is "unknown" if Mastercard is unable to readily determine a known at-risk time frame. In such event, an at-risk time frame for an Account number commences twelve (12) months prior to the date of publication of the first ADC Alert for the ADC Event or Potential ADC Event that discloses that Account number, and ends on the date specified in that ADC Alert. The number of days that the Issuer has to report fraudulent Transactions to the Fraud and Loss Database associated with an Account number disclosed in an ADC Alert is specified in the Alert; an Issuer is ineligible to receive FR associated with a fraudulent Transaction arising from use of an Account number if that fraudulent Transaction is not timely reported to the Fraud and Loss Database. Mastercard will determine the number of days that the Issuer has to report fraudulent Transactions to the Fraud and Loss Database for a disclosed Account number as follows:

- If Mastercard publishes an ADC Alert before Mastercard has received a final PFI report concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 30, 45, or 60 days to report fraudulent Transactions to the Fraud and Loss Database.

NOTE: As set forth in Chapter 5 of the *ADC User's Guide*, Mastercard determines the number of days in which an Issuer must report fraudulent Transactions to the Fraud and Loss Database based on the number of Accounts placed at risk in the ADC Event or Potential ADC Event: (i) if an ADC Event or Potential ADC Event placed 30,000 to 1,000,000 Accounts at risk, then the number of days will be 30; (ii) if an ADC Event or Potential ADC Event placed 1,000,000 to 5,000,000 Accounts at risk, then the number of days will be 45; or (iii) if an ADC Event or Potential ADC Event placed at least 5,000,000 Accounts at risk, then the number of days will be 60.

- If Mastercard publishes an ADC Alert after Mastercard has received a final PFI report concerning the ADC Event or Potential ADC Event and a previous ADC Alert concerning the ADC Event has been published by Mastercard, then that ADC Alert will specify whether the Issuer has 20, 35, or 50 days to report fraudulent Transactions to the Fraud and Loss Database.

  NOTE: As set forth in Chapter 5 of the *ADC User's Guide*, Mastercard determines the number of days in which an Issuer must report fraudulent Transactions to the Fraud and Loss Database based on the number of Accounts placed at risk in the ADC Event or Potential ADC Event: (i) if an ADC Event or Potential ADC Event placed 30,000 to 1,000,000 Accounts at risk, then the number of days will be 20; (ii) if an ADC Event or Potential ADC Event placed 1,000,000 to 5,000,000 Accounts at risk, then the number of days will be 35; or (iii) if an ADC Event or Potential ADC Event placed at least 5,000,000 Accounts at risk, then the number of days will be 50.

Accounts Disclosed for Different ADC Events

An Account number disclosed in an ADC Alert in connection with a different ADC Event during the 180 calendar days prior to the earliest disclosure of that Account number in an ADC Alert published in connection with the subject ADC Event is not eligible for ADC fraud recovery for the subject ADC Event.

Chargeback Deduction

In addition, a standard deductible, published from time to time, is applied to compensate for chargeback recoveries on Transactions using at-risk Account numbers.

Chip Liability Shift Impact

Account numbers with incremental counterfeit fraud that qualify for Issuer chargeback under message reason code 4870 or 70 (Chip Liability Shift) will be removed from consideration during the ADC fraud recovery calculation process.

For additional information regarding the criteria used by Mastercard in determining the at-risk time frame, refer to Chapter 5 of the *ADC User's Guide*.

United States Region Only—Mastercard will:

For an ADC Event investigation opened by Mastercard on or after 1 October 2013:

1. Halve the FR, if the compromised entity is a U.S. Region Acquirer's Merchant located in the U.S. Region and Mastercard determines that (i) at least seventy-five percent (75%) of the Merchant's annual total Transaction count was processed through Hybrid POS Terminals; and (ii) at least seventy-five percent (75%) of the Transactions deemed by Mastercard to be

within the scope of the ADC Event were processed through Hybrid POS Terminals; and (iii) the Merchant has not been identified by Mastercard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest ADC Alert for the subject ADC Event; and (iv) Mastercard determines that the Merchant was not storing Sensitive Authentication Data; or

2. Effective 1 October 2015, not assess FR if the compromised entity is a U.S. Region Acquirer's Merchant located in the U.S. Region and Mastercard determines that (i) at least ninety-five percent (95%) of the Merchant's annual total Transaction count was acquired through Hybrid POS Terminals; and (ii) at least ninety-five percent (95%) of the Transactions deemed by Mastercard to be within the scope of the ADC Event were acquired through Hybrid POS Terminals; and (iii) the Merchant has not been identified by Mastercard as having experienced a different ADC Event during the twelve (12) months prior to the date of publication of the earliest ADC Alert for the subject ADC Event; and (iv) Mastercard determines that the Merchant was not storing Sensitive Authentication Data.

   For purposes of this subsection, a Merchant's annual total Transaction count is determined based on the Merchant's clearing Transactions processed during the twelve (12) months prior to the date of publication of the ADC Alert through the GCMS. Transactions not processed by Mastercard are included in the annual Transaction count only if data pertaining to such Transactions is readily available to Mastercard. In the event that Mastercard is unable to readily determine the Merchant's actual annual total Transaction count, Mastercard may exercise its judgment to determine an annual total Transaction count. Mastercard may require an Acquirer to provide information to Mastercard for that purpose.

All Regions Other than the U.S. Region—For an ADC Event investigation opened by Mastercard on or after 1 December 2014, Mastercard will determine FR in the manner set forth in the subsection above pertaining to the U.S. Region, provided the requisite percentage of processed Transactions were processed through Hybrid POS Terminals.

10.7 Assessments and/or Disqualification for Noncompliance

If the Customer fails to comply with the procedures set forth in this Chapter 10, Mastercard may impose an assessment of up to USD 25,000 a day for each day that the Customer is noncompliant and/or disqualify the Customer from participating as a recipient of ADC operational reimbursement and fraud recovery disbursements, whether such disbursements are made in connection with the subject ADC Event or any other ADC Event, from the date that Mastercard provides the Customer with written notice of such disqualification until Mastercard determines that the Customer has resolved all compliance issues in this Chapter 10.

10.8 Final Financial Responsibility Determination

Upon completion of its investigation, if Mastercard determines that a Customer bears financial responsibility for an ADC Event or Potential ADC Event, Mastercard will notify the responsible Customer of such determination and, either contemporaneous with such notification or

thereafter, specify the amount of the Customer's financial responsibility for the ADC Event or Potential ADC Event.

The responsible Customer has thirty (30) calendar days from the date of such notification of the amount of the Customer's financial responsibility to submit a written appeal to Mastercard, together with any documentation and/or other information that the Customer wishes Mastercard to consider in connection with the appeal. Only an appeal that both contends that the Mastercard financial responsibility determination was not in accordance with the Standards and specifies with particularity the basis for such contention will be considered. Mastercard will assess a non-refundable USD 500 fee to consider and act on a request for review of an appeal.

If the appeal is timely and meets these criteria, Mastercard will consider the appeal and the documentation and/or other information submitted therewith in determining whether or not the Mastercard final financial responsibility determination was made in accordance with the Standards. An appeal that is not timely or does not meet these criteria will not be considered. The Mastercard decision with respect to an appeal is final and there are no additional internal appeal rights.

After reviewing the appeal, Mastercard will notify the responsible Customer of the appeal decision. If Mastercard denies or does not act on the appeal, Mastercard will debit the responsible Customer's MCBS account on the date specified in the appeal decision notification letter.

This section does not relieve a Customer of any responsibility set forth in sections 10.3 and 10.4, including the responsibility to submit to Mastercard on a continuing basis throughout the pendency of the Mastercard investigation the information required by those sections. If Mastercard determines that a Customer knew or should have known with reasonable diligence of documents or other information that the Customer was required to submit to Mastercard during the pendency of the Mastercard investigation in accordance with section 10.3 or 10.4, but failed to do so, such documents or other information will not be considered by Mastercard in deciding the appeal.

Chapter 11 MATCH System

This chapter is for Acquirer personnel responsible for investigating and signing potential new Merchants and for adding Merchants to the Mastercard Alert to Control High-risk (Merchants) (MATCH™) system.

11.1 MATCH Overview

The Mastercard Alert to Control High-risk (Merchants) (MATCH™) system is designed to provide Acquirers with the opportunity to develop and review enhanced or incremental risk information before entering into a Merchant Agreement. MATCH is a mandatory system for Mastercard Acquirers unless excused by Mastercard or prohibited by law. The MATCH database includes information about certain Merchants (and their owners) that an Acquirer has terminated.

When an Acquirer considers signing a Merchant, MATCH can help the Acquirer assess whether the Merchant was terminated by another Acquirer due to circumstances that could affect the decision whether to acquire for this Merchant and, if a decision is made to acquire, whether to implement specific action or conditions with respect to acquiring.

11.1.1 System Features

MATCH uses Customer-reported information regarding Merchants and their principal owners to offer Acquirers the following fraud detection features and options for assessing risk:

- Acquirers may add and search for information regarding up to five principal owners for each Merchant.
- MATCH uses multiple fields to determine possible matches.
- MATCH edits specific fields of data and reduces processing delays by notifying inquiring Customers of errors as records are processed.
- MATCH supports retroactive alert processing of data residing on the database for up to 360 days.
- Acquirers determine whether they want to receive inquiry matches, and if so, the type of information that the system returns.
- Acquirers may also access MATCH data in real time using MATCH Online or the Open Application Programming Interface (Open API).
- Acquirers may submit and receive bulk data using Batch and Import file operations.
- Acquirers may add and search for information regarding Merchant uniform resource locator (URL) website addresses.

Through the MATCH system, an inquiring Acquirer may determine whether the Merchant inquired of is the same Merchant previously reported to MATCH, terminated, or inquired about within the past 360 days. The inquiring Acquirer must then determine whether additional investigation is appropriate, or if it should take other measures to address risk issues.

11.1.2 How does MATCH search when conducting an inquiry?

MATCH searches the database for possible matches between the information provided in the inquiry and the following:

- Information reported and stored during the past five years
- Other inquiries during the past 360 days

MATCH searches for exact possible matches and phonetic possible matches.

NOTE: All MATCH responses reflecting that inquiry information is resident on MATCH are deemed "possible matches" because of the nature of the search mechanisms employed and the inability to report a true and exact match with absolute certainty.

NOTE: There are two types of possible matches, including a data match (for example, name-to-name, address-to-address) and a phonetic (sound-alike) match made using special software.

NOTE: For convenience only, the remainder of this manual may sometimes omit the word "possible" when referring to "possible matches" or "a possible match."

The Acquirer determines the number of phonetic matches—one to nine—that will cause a possible match to be trustworthy.

MATCH returns the first 100 responses for each inquiry submitted by an Acquirer. MATCH returns all terminated Merchant MATCH responses regardless of the number of possible matches.

11.1.2.1 Retroactive Possible Matches

If the information in the original inquiry finds new possible matches of a Merchant or inquiry record in the MATCH database added since the original inquiry was submitted and this information has not been previously reported to the Acquirer at least once within the past 360 days, the system returns a **retroactive** possible match response.

11.1.2.2 Exact Possible Matches

MATCH finds an exact possible match when data in an inquiry record matches data on the MATCH system letter-for-letter, number-for-number, or both. An exact match to any of the following data results in a possible match response from Mastercard.

Table 11.1—Exact Possible Match Criteria

Field	+	Field	+	Field	=	Match
Merchant Name					=	√
Doing Business as (DBA) Name					=	√
Phone Number (Merchant)					=	√
Alternate Phone Number (Merchant)					=	√
Merchant National Tax ID	+	Country			=	√
Merchant State Tax ID	+	State			=	√
Merchant Street Address	+	City	+	State[1]	=	√

[1] If country is USA.

Field	+	Field	+	Field	=	Match
Merchant Street Address	+	City	+	Country[2]	=	√
Merchant URL Website Address	+	City	+	Country	=	√
Principal Owner's (PO) First Name	+	Last Name			=	√
PO Phone Number					=	√
Alternate Phone Number (PO)					=	√
PO Social Security Number[1]					=	√
PO National ID[2]					=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO State[1]	=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO Country[2]	=	√
PO Driver's License (DL) Number	+	DL State[1]			=	√
PO Driver's License Number	+	DL Country[2]			=	√

NOTE: MATCH uses Street, City, and State if the Merchant's country is USA; otherwise, Street, City, and Country are used.

NOTE: Acquirers must populate the Merchant URL Website Address field when performing an inquiry of an electronic commerce (e-commerce) Merchant.

11.1.2.3 Phonetic Possible Matches

The MATCH system converts certain alphabetic data, such as Merchant Name and Principal Owner Last Name to a phonetic code. The phonetic code generates matches on words that sound alike, such as "Easy" and "EZ." The phonetic matching feature of the system also matches names that are not necessarily a phonetic match but might differ because of a typographical error, such as "Rogers" and "Rokers," or a spelling variation, such as "Lee," "Li," and "Leigh."

MATCH evaluates the following data to determine a phonetic possible match.

Table 11.2—Phonetic Possible Match Criteria

Field	+	Field	+	Field	=	Match
Merchant Name					=	√
Doing Business As (DBA) Name					=	√

[2] If country is not USA.

Field	+	Field	+	Field	=	Match
Merchant Street Address	+	City	+	State[3]	=	√
Merchant Street Address	+	City	+	Country[4]	=	√
Principal Owner's (PO) First Name	+	Last Name			=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO State[3]	=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO Country[4]	=	√

NOTE: MATCH uses Street, City, and State if the Merchant's country is USA; otherwise, Street, City, and Country are used.

11.2 MATCH Standards

Mastercard mandates that all Acquirers with Merchant activity use MATCH.[5] To use means both to:

- Add information about a Merchant that is terminated while or because a circumstance exists (See section 11.2.2), and
- Inquire against the MATCH database

Customers must act diligently, reasonably, and in good faith to comply with MATCH Standards.

11.2.1 Certification

Each Acquirer that conducts Merchant acquiring Activity must be certified by Mastercard to use MATCH because it is a mandatory system. An Acquirer that does not comply with these requirements may be assessed for noncompliance, as described in this chapter.

Certification is the process by which Mastercard connects an Acquirer to the MATCH system, so that the Acquirer may send and receive MATCH records to and from Mastercard. To be certified for MATCH usage, Acquirers must request access for each Member ID/ICA number under which acquiring Activity is conducted.

NOTE: An Acquirer that conducts Merchant acquiring Activity under a Member ID/ICA number that does not have access to the MATCH system is not considered certified.

An Acquirer that is not MATCH-certified is subject to noncompliance assessments as described in Table 11.3.

[3] If country is USA.
[4] If country is not USA.
[5] Acquirers globally are assessed an annual MATCH usage fee of USD 5,000. In addition, Acquirers are assessed a MATCH inquiry fee (per Member ID/ICA number) for each MATCH inquiry.

11.2.2 When to Add a Merchant to MATCH

If either the Acquirer or the Merchant acts to terminate the acquiring relationship (such as by giving notice of termination) and, at the time of that act, the Acquirer has reason to believe that a condition described in Table 11.4 exists, then the Acquirer must add the required information to MATCH within five calendar days of the earlier of either:

1. A decision by the Acquirer to terminate the acquiring relationship, regardless of the effective date of the termination, or
2. Receipt by the Acquirer of notice by or on behalf of the Merchant of a decision to terminate the acquiring relationship, regardless of the effective date of the termination.

Acquirers must act diligently, reasonably, and in good faith to comply with MATCH system requirements.

Acquirers may not use or threaten to use MATCH as a collection tool for minor Merchant discretionary activity. One of the defined reason codes in Table 11.4 must be met or suspected (at decision to terminate) to justify a Merchant addition. Acquirers that use or threaten to use MATCH as a collection tool for minor Merchant discretionary activity are subject to noncompliance assessments as described in Table 11.3.

An Acquirer that fails to enter a Merchant into MATCH is subject to a noncompliance assessment, and may be subject to an unfavorable ruling in a compliance case filed by a subsequent Acquirer of that Merchant.

11.2.3 Inquiring about a Merchant

An Acquirer must check MATCH **before** signing an agreement with a Merchant and/or enabling a Merchant to accept Transactions, in accordance with section 7.1 of this manual.

An Acquirer that enters into a Merchant Agreement without first submitting an inquiry to MATCH about the Merchant may be subject to an unfavorable ruling in a compliance case filed by a subsequent Acquirer of that Merchant.

Acquirers must conduct inquiries under the proper Member ID/ICA Number for reporting compliance reasons. If an Acquirer does not conduct the inquiry under the proper Member ID/ICA Number (that is, the Member ID/ICA Number that is actually processing for the Merchant), Mastercard may find the Acquirer in noncompliance and may impose an assessment.

Failure to comply with either the requirement of adding a terminated Merchant or inquiring about a Merchant may result in noncompliance assessments as described in Table 11.3.

11.2.6 MATCH Record Retention

Merchant records remain on the MATCH system for five years, at which point they are automatically purged from the MATCH system. The Acquirer must retain all MATCH records concerning a Merchant, Sponsored Merchant, or ATM owner for a minimum of two years after the data that the Merchant Agreement, Sponsored Merchant Agreement, or ATM Owner Agreement, as applicable, is terminated or expires.

NOTE: The MATCH system database stores inquiry records for 360 days.

11.4 Merchant Removal from MATCH

Mastercard may remove a Merchant listing from MATCH for the following reasons:

- The Acquirer reports to Mastercard that the Acquirer added the Merchant to MATCH in error.
- The Merchant listing is for reason code 12 (*Payment Card Industry Data Security Standard* Noncompliance) and the Acquirer has confirmed that the Merchant has become compliant with the *Payment Card Industry Data Security Standard*. The Acquirer must submit the request to remove a MATCH reason code 12 Merchant listing from MATCH in writing on the Acquirer's letterhead to matchbusinessowner@mastercom.com. Such request must include the following information:
  1. Acquirer ID Number
  2. Merchant ID Number
  3. Merchant Name
  4. Doing Business As (DBA) Name
  5. Business Address
     a. Street Address
     b. City
     c. State
     d. Country
     e. Postal Code
  6. Principal Owner (PO) Data
     a. PO's First Name and Last Name
     b. PO's Country of Residence

     Any request relating to a Merchant listed for reason code 12 must contain:

     – The Acquirer's attestation that the Merchant is in compliance with the *Payment Card Industry Data Security Standard*, and
     – A letter or certificate of validation from a Mastercard certified forensic examiner, certifying that the Merchant has become compliant with the *Payment Card Industry Data Security Standard*.

     If an Acquirer is unwilling or unable to submit a request to Mastercard with respect to a Merchant removal from a MATCH listing as a result of the Merchant obtaining compliance with the *Payment Card Industry Data Security Standard*, the Merchant itself may submit a request to Mastercard for this reason. The Merchant must follow the same process as described above for Acquirers to submit the MATCH removal request.

11.5 MATCH Reason Codes

MATCH reason codes identify whether a Merchant was added to the MATCH system by the Acquirer or by Mastercard, and the reason for the listing.

11.5.1 Reason Codes for Merchants Listed by the Acquirer

The following reason codes indicate why an Acquirer reported a terminated Merchant to MATCH.

Table 11.4—MATCH Listing Reason Codes Used by Acquirers

MATCH Reason Code	Description
01	***Account Data Compromise*** An occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of Account data.
02	***Common Point of Purchase (CPP)*** Account data is stolen at the Merchant and then used for fraudulent purchases at other Merchant locations.
03	***Laundering*** The Merchant was engaged in laundering activity. Laundering means that a Merchant presented to its Acquirer Transaction records that were not valid Transactions for sales of goods or services between that Merchant and a bona fide Cardholder.
04	***Excessive Chargebacks*** With respect to a Merchant reported by a Mastercard Acquirer, the number of Mastercard chargebacks in any single month exceeded 1% of the number of Mastercard sales Transactions in that month, and those chargebacks totaled USD 5,000 or more. With respect to a merchant reported by an American Express acquirer (ICA numbers 102 through 125), the merchant exceeded the chargeback thresholds of American Express, as determined by American Express.
05	***Excessive Fraud*** The Merchant effected fraudulent Transactions of any type (counterfeit or otherwise) meeting or exceeding the following minimum reporting Standard: the Merchant's fraud-to-sales dollar volume ratio was 8% or greater in a calendar month, and the Merchant effected 10 or more fraudulent Transactions totaling USD 5,000 or more in that calendar month.
06	***Reserved for Future Use***

MATCH Reason Code	Description
08	***Mastercard Questionable Merchant Audit Program*** The Merchant was determined to be a Questionable Merchant as per the criteria set forth in the Mastercard Questionable Merchant Audit Program (refer to section 8.4 of this manual).
09	***Bankruptcy/Liquidation/Insolvency*** The Merchant was unable or is likely to become unable to discharge its financial obligations.
10	***Violation of Standards*** With respect to a Merchant reported by a Mastercard Acquirer, the Merchant was in violation of one or more Standards that describe procedures to be employed by the Merchant in Transactions in which Cards are used, including, by way of example and not limitation, the Standards for honoring all Cards, displaying the Marks, charges to Cardholders, minimum/maximum Transaction amount restrictions, and prohibited Transactions set forth in Chapter 5 of the *Mastercard Rules* manual. With respect to a merchant reported by an American Express acquirer (ICA numbers 102 through 125), the merchant was in violation of one or more American Express bylaws, rules, operating regulations, and policies that set forth procedures to be employed by the merchant in transactions in which American Express cards are used.
11	***Merchant Collusion*** The Merchant participated in fraudulent collusive activity.
12	***PCI Data Security Standard* Noncompliance** The Merchant failed to comply with *Payment Card Industry (PCI) Data Security Standard* requirements.
13	***Illegal Transactions*** The Merchant was engaged in illegal Transactions.
14	***Identity Theft*** The Acquirer has reason to believe that the identity of the listed Merchant or its principal owner(s) was unlawfully assumed for the purpose of unlawfully entering into a Merchant Agreement.

11.7 Legal Notice

11.7.1 Privacy and Data Protection

An Acquirer that stores, transmits, or processes Personal Data[6], of a resident of the European Economic Area, the UK, or Switzerland or that is otherwise subject to EU Data Protection Law[6] must comply with the Standards set forth in Appendix D of this manual pertaining to MATCH Activity conducted in the Europe Region.

[6] This capitalized term has the meaning set forth in Appendix D of this manual. All other capitalized terms used in this manual are defined in the Definitions appendix (Appendix E) of this manual.

Chapter 12 Omitted

This chapter has been omitted.

Chapter 13 Franchise Management Program

This chapter describes the Franchise Management Program Standards and applies to all Mastercard Customers, Service Providers, and Payment Facilitators.

13.1 About the Franchise Management Program

The Franchise Management Program is dedicated to supporting healthy Customer and Service Provider growth. The program works with Customers and Service Providers to ensure that they understand and operate within the Standards to minimize operational, financial, reputational, and compliance risks.

In addition, the Franchise Management Program provides industry best practices to support business growth by enhancing the overall operational efficiency and profitability of the issuing and acquiring Portfolio while maintaining losses at an acceptable level.

The Franchise Management Program consists of three mandatory levels and one optional level. The three mandatory levels are:

- **Customer Onboarding Reviews** for prospective Mastercard Principal Customers and Affiliate Customers;
- The **Service Provider Risk Management Program**; and
- **Customer Franchise Reviews** for Mastercard Customers. A Maestro Customer identified by Mastercard as a Group 3 Issuer pursuant to the Maestro Issuer Loss Control Program (LCP) may also be required to undergo a Customer Franchise Review.

A Customer may also choose to participate in **Customer Consultative Reviews**.

This chapter describes the Standards for each review level.

13.1.2 Service Provider Risk Management Program

The Service Provider Risk Management Program addresses the risks to which a Service Provider may be exposed on an ongoing basis.

Following Service Provider registration, Mastercard segments the Service Provider's Portfolio to determine the entity's level of risk based on the types of services that the entity provides and its potential level of exposure to the Mastercard Network.

Based on the results of this segmentation, Mastercard determines the most appropriate approach for evaluating the Service Provider's level of risk. These evaluations may include, but are not be limited to:

- Requesting information directly from the Service Provider to help determine the entity's risk profile and its ability to support Mastercard Customers; and
- Performing a remote questionnaire review or an onsite review to evaluate the controls that the Service Provider has in place to mitigate risks.

Mastercard reserves the right for Franchise Management Program staff to conduct a review of any Service Provider at any time.

Mastercard may provide a summary of the results of its review to any Customer that has registered the Service Provider. A Service Provider that fails either or both of the following Mastercard requirements may be subject to de-registration as a Service Provider:

- Demonstration to the satisfaction of Mastercard that the entity has adequate and effective controls in place to mitigate risk; and
- Adherence to a Mastercard-approved action plan.

Topics covered during a Service Provider Risk Management Program review are listed in section 13.2.

The Customer must at all times be entirely responsible for and must manage, direct, and control all aspects of its Program and Program Service performed by Service Providers, and establish and enforce all Program management and operating policies in accordance with the Standards according to Rule 7.2.1 of the *Mastercard Rules* manual.

The completion of a Service Provider Risk Management Program review does not imply, suggest, or otherwise mean that Mastercard endorses the Service Provider or the nature or quality of Program Service or other performance or that Mastercard approves of, is a party to, or a participant in, any act or omission by a Service Provider or other entity acting for or on behalf of a Customer.

Refer to Chapter 7 of the *Mastercard Rules* manual for more information about Service Provider requirements.

Appendix A Omitted

This appendix has been omitted.

Appendix B Omitted

This appendix has been omitted.

Appendix C Omitted

This appendix has been omitted.

Appendix D Covered Programs Privacy and Data Protection Standards

This appendix describes the privacy and data protection Standards for Covered Programs as they relate to European Union (EU) Data Protection Law.

D.1 Purpose

This appendix provides Standards regarding the Processing of Personal Data of Data Subjects subject to EU Data Protection Law by the Corporation and its Customers (collectively referred to in this appendix as the "Parties") in the context of the Covered Programs: Account Data Compromise events, Mastercard Alert to Control High-risk (Merchants) (MATCH™) system, the Excessive Chargeback Program, the Merchant Registration Program, and the Franchise Management Program.

D.2 Scope

The Standards in this appendix supplement the privacy and data protection Standards contained in Section 1.5 of this manual and Rule 3.13 of the *Mastercard Rules* to the extent that the requirements pertain to the Processing of Personal Data subject to EU Data Protection Law in the context of the Covered Programs. In the event of a conflict, the Standards in this appendix take precedence.

D.3 Definitions

As used solely for the purposes of this appendix, the following terms have the meanings set forth below. Capitalized terms not otherwise defined herein have the meaning provided in Appendix E of this manual.

Controller

The entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

Criminal Data

Any Personal Data relating to criminal convictions, offenses, or related security measures.

EEA Standard Contractual Clauses (EEA SCCs)

The clauses annexed to the EU Commission Decision 2021/914 of June 4, 2021, on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as amended from time to time.

EU Data Protection Law

The EU General Data Protection Regulation 2016/679 GDPR (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); the Monaco Data Protection Act 2018 (as amended and replaced from time to time); the UK Data

Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the EEA countries (as amended and replaced from time to time).

Mastercard Binding Corporate Rules (Mastercard BCRs)

The Mastercard Binding Corporate Rules as approved by the EEA and UK data protection authorities and available on the Corporation's public facing website.

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.

UK Addendum

The addendum to the EEA Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).

D.4 Acknowledgment of Roles

The Corporation and its Customers acknowledge and confirm that: (1) neither Party acts as a Processor on behalf of the other Party; (2) each Party is an independent Controller; and (3) this appendix does not create a joint-Controllership or a Controller-Processor relationship between the Parties. The Corporation and its Customers acknowledge and agree that the scope of each Party's role as an independent Controller is as follows:

- A Customer is a Controller for any Processing, including disclosing Personal Data to the Corporation, for the purpose of developing enhanced or incremental risk information to aid the Customer in its own determination of risk in its Merchant acquiring business.
- The Corporation is a Controller for any Processing for the purpose of operating the Covered Programs, including product development, support and maintenance, and making the Covered Programs available to its Customers (e.g., as set out in Chapter 11) and for internal research, fraud, security, and risk management as listed in Rule 3.10 "Confidential Information of Customers" of the *Mastercard Rules*.

D.5 The Corporation and Customer Obligations

The Corporation and each Customer independently is responsible for compliance with EU Data Protection Law in relation to the Processing of Personal Data for which it is a Controller as described in section D.4.

Notwithstanding the above, with regard to any Processing of Personal Data of Data Subjects that a Customer adds to the Covered Programs, including the Processing for which the Corporation is the Controller, a Customer must:

1. Rely on a valid legal ground under EU Data Protection Law for each of the Processing purposes, including obtaining Data Subjects' consent if required or appropriate under EU Data Protection Law.
2. Provide appropriate notice to the Data Subjects regarding (i) the their Processing of Personal Data, in a timely manner (e.g., informing Merchants about the possible use of MATCH upon termination of the Merchant Agreement) and at the minimum with the elements required under EU Data Protection Law, and (ii), as appropriate, the existence of Mastercard BCRs. Each Customer must also provide a link to the Corporation's privacy notice for the Processing in relation to MATCH (available at https://www.mastercard.com/global/en/vision/corp-responsibility/commitment-to-privacy/match-privacy.html), where applicable.
3. Take reasonable steps to ensure that Personal Data are accurate, complete, and current; adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed.
4. Respond to Data Subjects' requests to exercise their rights under EU Data Protection Law, including the right of (i) access, (ii) rectification, (iii) erasure, (iv) data portability, (v) restriction of Processing, and (vi) objection to the Processing, if and as required under EU Data Protection Law. The Corporation agrees to cooperate with the Customer in responding to such requests where appropriate.
5. Limit its Processing of Personal Data to the Processing that is necessary for the purpose of developing enhanced or incremental risk information to aid in its own determination of risk in its Merchant acquiring business.
6. Not engage in or otherwise perform any automated decision-making or profiling based on Personal Data that are Processed in the context of the Covered Programs.
7. Will add any Sensitive Data, Criminal Data, or government identification information of Data Subjects to the Covered Programs.
8. Only Process Personal Data in connection with the Covered Programs for as long as necessary to achieve the purposes for which they are Processed. Any Personal Data Processed in relation to MATCH must be deleted or destroyed after a maximum of five (5) years.

D.6 Data Transfers

A Customer may transfer the Personal Data Processed in connection with the Covered Programs outside of the EEA, the UK, and Switzerland in accordance with EU Data Protection Law, including based on the EEA SCCs or the UK Addendum as appropriate.

The Corporation may transfer the Personal Data Processed in connection with the Covered Programs outside of the EEA, the UK, and Switzerland 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. The Corporation will abide by the Mastercard BCRs when Processing Personal Data in the context of the Covered Programs.

D.7 Data Disclosures

The Corporation and its Customers must ensure that they will only disclose Personal Data Processed in the context of the Covered Programs in accordance with EU Data Protection Law, and in particular that they will require the data recipients to protect the data with at least the same level of protection as described in this appendix. The Corporation represents and warrants that it will only disclose Personal Data in accordance with the Mastercard BCRs.

Where the Corporation transfers Personal Data subject to the GDPR or the Swiss Data Protection Act to a Customer in a country that is not part of the EEA or subject to a European Commission adequacy decision, the Parties agree that the transfer shall be governed by the EEA SCCs, which are hereby incorporated into this appendix by reference. The SCCs are completed as follows: the Parties conclude Module One (controller-to-controller) of the EEA SCCs. The "data exporter" is Corporation; the "data importer" is Customer; the optional docking clause in Clause 7 is implemented; the optional paragraph in Clause 11(a) is struck; the competent supervisory authority in Clause 13(a) shall be the supervisory authority of Belgium; the governing law in Clause 17 is the law of the Belgium and the courts in Clause 18(b) are the courts of the Belgium; Annex 1 and 2 to the EEA SCCs are Annex 1 and 2 to this appendix.

The Parties conclude the UK Addendum for transfers of Personal Data subject to the UK Data Protection Act from Corporation to Customer in a country that is not subject to a UK adequacy decision. The UK Addendum is hereby incorporated into this appendix by reference. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Corporation and the "Importer" is Customer (as set out in the paragraph above), their details are set forth in the Acquirer license agreement and their signatures are included in the signature page of the Acquirer license agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are those incorporated into this appendix as per the paragraph above; (iii) in Table 3, Annexes 1 and 2 to the Approved EU SCCs are Annexes 1 and 2 to this appendix respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

If either Party's compliance with EU Data Protection Law applicable to transfers of Personal Data is affected by circumstances outside of either Party's control, including if a legal

instrument for transfers is invalidated, amended, or replaced, then the Parties will work together in good faith to reasonably resolve such non-compliance.

D.8 Security Measures

The Corporation and its Customers 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, which includes, at a minimum, as appropriate: (1) the pseudonymization and encryption of Personal Data; (2) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; (3) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (4) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

In assessing the appropriate level of security, the Corporation and its Customers 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.

D.9 Confidentiality of Personal Data

The Corporation and its Customers 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 if applicable, Process Personal Data in accordance with the Controller's instructions.

D.10 Personal Data Breach Notification Requirements

The Parties will assist each other in complying with their Personal Data Breach notification obligations. Where required under EU Data Protection Law, the Party which became aware of a Personal Data Breach will notify, without undue delay and, where feasible, not later than 72 hours after having become aware of it, the competent supervisory authority.

When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects or upon the competent supervisory authority's request to do so, such Party must communicate the Personal Data Breach to the Data Subject without undue delay, where required under EU Data Protection Law.

D.11 Personal Data Breach Cooperation and Documentation Requirements

Each Party must notify the other Party of a Personal Data Breach that relates to Personal Data Processed in the context of the Covered Programs and for which the other Party is a Controller, without undue delay, and not later than forty-eight (48) hours after having become aware of a Personal Data Breach. Each Party must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects, and the remedial action taken.

D.12 Data Protection and Security Audit

The Corporation and each Customer must conduct audits on a regular basis to control compliance with EU Data Protection Law, including the security measures provided in section D.8, and the Corporation must comply with the Mastercard BCRs.

Upon prior written request, the Corporation and each Customer agrees to cooperate and, within reasonable time, provide the requesting Party with: (1) a summary of the audit reports demonstrating its compliance with EU Data Protection Law obligations and the Standards in this appendix, and as applicable Mastercard BCRs, after redacting any confidential and commercially sensitive information; and (2) confirmation that the audit has not revealed any material vulnerability, or to the extent that any such vulnerability was detected, that such vulnerability has been fully remedied.

D.13 Liability

Subject to the liability clauses in the Standards, the Corporation and each Customer agrees that it will be liable towards Data Subjects for the entire damage resulting from a violation of EU Data Protection Law with regard to Processing of Personal Data for which it is a Controller.

Where the Parties are involved in the same Processing and where they are responsible for any damage caused by the Processing of Personal Data, both the Corporation and each responsible Customer 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, the Corporation is entitled to claim back from the Customer(s) that part of the compensation corresponding to each Customer's part of responsibility for the damage.

D.14 Termination of the Covered Programs Use

Mastercard and its Customers agree that, apart from the data retention obligation in section D.5, paragraph 8, the Standards in this appendix are no longer applicable to a Customer upon the termination of such Customer's use of the Covered Programs.

D.15 Invalidity and Severability

If any Standard in this appendix is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such Standard shall not affect any other Standard in this appendix, and all Standards not affected by such invalidity or unenforceability will remain in full force and effect.

Annex 1 to Appendix D: 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 Acquirer License agreement.
   - Activities relevant to the data transferred: Providing the Covered Programs
   - Signature and date: as stipulated in the Acquirer License agreement
   - Role: controller for the purposes listed in Section D.4 of appendix D.
2. **Data importer: Customer**
   - Name and address of the Customer as well as the name, position, and contact details for Customer's contact person: as stipulated in the Acquirer License agreement
   - Activities relevant to the data transferred: participating in, or benefiting from, the Covered Programs
   - Signature and date: as stipulated in the Acquirer License agreement
   - Role: controller for the purposes listed in Section D.4 of appendix D

B. Description of the Transfer

Data Subjects

Data Subjects as defined in Appendix E.

Categories of data

Personal Data relating to a Merchant's principal owners or sole proprietors.

Sensitive Data transferred

The Parties do not Process any Sensitive Data in the context of the Covered Programs.

Frequency of the transfer

Upon Customer's requests, such as on a per query basis or via batch file transfer.

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 D.4 of appendix D.

Period for which the Personal Data will be retained

Personal Data will be retained only for as long as necessary to achieve the relevant purposes for each of the Covered Programs.

C. Competent Supervisory Authority

The competent supervisory authority in accordance with Clause 13 of the EEA SCCs is the Belgian Data Protection Authority.

Annex 2 to Appendix D: Technical and Organizational Measures Ensure the Security of the Data

The Parties will, as a minimum, implement the following types of security measures:

1. **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, include:
   - Establishing security areas, restriction of access paths;
   - Establishing access authorizations for employees and third parties;
   - Access control system (ID reader, magnetic card, chip card);
   - Key management, card-keys procedures;
   - Door locking (electric door openers, etc.);
   - Security staff, janitors;
   - Surveillance facilities, video/CCTV monitor, alarm system;
   - Securing decentralized data processing equipment and personal computers.
2. **Virtual access control**
   Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:
   - User identification and authentication procedures;
   - ID/password security procedures (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;
- Creation of one master record per user, user master data procedures, per data processing environment.

3. **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, include:

   - Internal policies and procedures;
   - Control authorization schemes;
   - Differentiated access rights (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;
   - Deletion procedure.

4. **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, include:

   - Tunneling
   - Logging
   - Transport security

5. **Entry control**
   Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

   - Logging and reporting systems;
   - Audit trails and documentation.

6. **Control of instructions**
   Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

   - Unambiguous wording of the contract;
   - Formal commissioning (request form);
   - Criteria for selecting the Processor

7. **Availability control**
   Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

   - Backup procedures;

- Mirroring of hard disks (e.g., RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. **Separation control**
   Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

   - Separation of databases;
   - "Internal client" concept / limitation of use;
   - Segregation of functions (production/testing);
   - Procedures for storage, amendment, deletion, transmission of data for different purposes.

Appendix E 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.

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 Enablement System

Performs Account enablement services for Mastercard Cloud-Based Payments, which may include Account and Access Device eligibility checks, Identification & Verification (ID&V), Digitization, and subsequent lifecycle management.

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.

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).

Authenticating Entity

An Authenticating Entity is a Merchant, Service Provider, or Digital Wallet Operator that uses an MFA Method to authenticate a Cardholder when a Token is used to conduct a Card-not-present Transaction of any type (excluding mail order and telephone order [MO/TO] Transactions).

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.

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:

- The comparison, by the Merchant or Acquirer accepting the Card, of the signature on the Card's signature panel with the signature provided on the Transaction receipt by the person presenting the Card;
- 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
- The use of a Consumer Device CVM (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 Quick Payment Service (QPS) Transactions, 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.

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 or No CVM Required 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, translated from English into another language, or appear in another alphabet except for specific authorized versions in Chinese (translation), Arabic (transliteration), Georgian (transliteration), and Korean (transliteration). 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 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 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 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 System

The Interchange System as defined in this manual.

Credentials Management System

Facilitates credential preparation and/or remote mobile Payment Application management for Mastercard Cloud-Based Payments.

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 DSE Program Service.

Data Subject

A Cardholder, a Merchant, or other natural person or entity whose Personal Data are Processed by or on behalf of the Corporation, a Customer, or a Merchant.

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 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 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.

Electronic Money Issuer

An Electronic Money Institution with respect only to its issuing activities.

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.

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 via the Corporation's Global Clearing Management System (GCMS), in accordance with the requirements set forth in the *Mastercard Global Collection Only* manual.

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.

Independent Sales Organization (ISO)

A Service Provider that performs 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), and the Settlement Account Management (SAM) system.

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.

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, via 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, translated from English into another language, or appear in another alphabet except for specific authorized versions in Chinese (translation), Arabic (transliteration), Georgian (transliteration), and Korean (transliteration). 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.

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, 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* 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, translated from English into another language, or appear in another alphabet except for specific authorized versions in Chinese (translation), Arabic (transliteration), Georgian (transliteration), and Korean (transliteration). 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 Token Requestor

A Merchant Token Requestor is a Merchant 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 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 via 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.

Multi-Factor Authentication Method, MFA Method

A Multi-Factor Authentication (MFA) Method is an authentication solution that includes two or more factors from the following categories: possession, knowledge, or inherence, with no more than one factor in any single category.

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, 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.

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 Sponsored Merchant, and upon the performance of a Transaction, transfers the Account data to the Merchant or Sponsored Merchant 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 Sponsored Merchant, and which in doing so, performs 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, 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 is 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 Manual Cash Disbursement Transaction. A POS Transaction 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 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 via 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 via the Corporation System, for the purpose of a transfer of funds via 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.

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 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, the Mastercard Send Cross-Border Service, 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. See Appendix A of the *Mastercard Rules* manual.

Remote Electronic Transaction

In the Europe Region, all types of Card-not-present Transaction (e-commerce Transactions, recurring payments, installments, Card-on-file Transactions, in-app Transactions, and Transactions completed through a Digital Wallet, including MasterPass™). Mail order and telephone order (MO/TO) Transactions and Transactions completed with anonymous prepaid Cards are excluded from this definition.

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.

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.

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. A Sponsored Merchant is also referred to as a 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. A Sponsored Merchant Agreement is also referred to as a Submerchant Agreement.

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 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.

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 via the Interchange System or otherwise) or that the Corporation requires to be provided.

Transaction Management System

Performs Transaction management services for Mastercard Cloud-Based Payments, which may include credential authentication, application cryptogram mapping and validation, ensuring synchronization with the Credentials Management System, and forwarding of Transactions to the Issuer for authorization.

Trusted Service Manager

Provisions an Access Device with the Payment Application, personalization data, or post-issuance application management commands by means of an over-the-air (OTA) communication channel.

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.

EMV® is a registered trademark of EMVCo LLC in the United States and other countries. For more information, see http://www.emvco.com.

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.