Security Rules and Procedures

Merchant Edition

25 September 2018

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
2.3	Contracting with Card Registration Companies	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 Member Information tool on Mastercard Connect™.

Chapter 2 Omitted

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

Any such consumer authentication technology must be approved by Mastercard as a "Mastercard-qualified CVM" before it may be used as a Consumer Device Cardholder Verification Method (CDCVM) to process a Transaction.

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 Mastercard by the Customer for certification and testing.

Certification and testing of a proposed CDCVM is performed by or on behalf of Mastercard, in accordance with Mastercard requirements and at the expense of the Customer or third party, as applicable. Certification requires both successful security and functional testing.

Upon the completion of certification and testing, Mastercard, in its discretion, may approve a proposed consumer authentication technology as a "Mastercard-qualified CVM." Summary report information about such certification and testing results and the successful completion of certification testing may be disclosed to Customers by Mastercard or a third party that conducts certification and testing on Mastercard's behalf. Any proposed update, change, or modification of the consumer authentication technology that could impact the functionality or security of the CDCVM must be submitted to Mastercard for certification and testing as a newly proposed consumer authentication technology. Mastercard reserves the right to change the requirements for a Mastercard-qualified CVM at any time, and to establish new or change certification and testing requirements.

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 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.

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.

3.12.4 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.

All non-face-to-face gambling Transactions conducted with a Mastercard Card must include the CVC 2 value in DE 48, subelement 92 of the Authorization Request/0100 message.

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, Mastercard Electronic, 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, Mastercard Electronic, 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 must be used on Mastercard Electronic™ Cards, but 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 and PIN Security Standards

This chapter may be of particular interest to Issuers of Cards that support PIN as a Cardholder Verification Method (CVM) and Acquirers of Terminals that accept PIN as a CVM. 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)

An Issuer must give each of its Cardholders a personal identification number (PIN) in conjunction with Mastercard Card issuance, or offer the Cardholder the option of receiving a PIN. The Issuer must give the Cardholder a PIN in conjunction with Maestro Card and Cirrus Card issuance. The 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.

An Issuer should refer to the guidelines for PIN and key management set forth in the *Issuer PIN Security Guidelines*.

An Acquirer must comply with the latest edition of the following documents, available at www.pcisecuritystandards.org:

- *Payment Card Industry PIN Security Requirements*
- *Payment Card Industry POS PIN Entry Device Security Requirements*
- *Payment Card Industry Encrypting PIN Pad Security Requirements*

4.3 PIN Verification

An Issuer must be capable of verifying PINs based on a maximum of six characters. The Issuer may use the PIN verification algorithm of its choice.

If a Card is encoded with a PIN Verification Value (PVV), then the Issuer may use the Mastercard PIN verification service for authorization processing. If a proprietary algorithm is used for the PVV calculation or the PVV is not encoded on the Card, then PIN verification will not be performed on a Transaction authorized by means of the Stand-In Processing Service.

A Customer in a Region other than the Europe Region may refer to "PIN Processing for Non-Europe Region Customers" in the *Authorization Manual*, Chapter 9, "Authorization Services Details" for more information about the Mastercard PIN verification service, in which the Mastercard Network performs PIN verification on behalf of Card Issuers. Europe Region Customers should refer to Chapter 12, "PIN Processing for Europe Region Customers," of the *Authorization Manual*.

Refer to "PIN Generation Verification" in *Single Message System Specifications*, Chapter 7, "Encryption" for more information about PIN verification that the Mastercard Network performs directly for Debit Mastercard Card and Maestro and Cirrus Card Issuers, and the two PIN verification methods (IBM 3624 and ABA) that the PIN verification service supports. The ANSI format of PIN block construction is also described in that chapter.

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*.

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

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 under Triple Data Encryption Standard (DES) software routines.
3. Use the Triple DES algorithm to perform all encryption.

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 PIN at the Point of Interaction (POI) for Mastercard Magnetic Stripe Transactions

Mastercard may authorize the use of a PIN for Mastercard magnetic stripe Transactions at selected Merchant types, POS Terminal types, or Merchant locations in specific countries. Mastercard requires the use of a PIN at CAT 1 devices. Acquirers and Merchants that support PIN-based Mastercard magnetic stripe Transactions must provide Cardholders with the option of a signature-based Transaction, unless the Transaction occurs at a CAT 1 device or at a CAT 3 device with offline PIN capability for Chip Transactions.

Mastercard requires Merchants to provide a POS Terminal that meets specific requirements for PIN processing wherever an approved implementation takes place. When applicable, each Transaction must be initiated with a Card in conjunction with the PIN entered by the Cardholder at the Terminal. The Acquirer must be able to transmit the PIN in the Authorization Request/0100 message in compliance with all applicable PIN security Standards.

Acquirers and Merchants must not require a Cardholder to disclose his or her PIN, other than by private entry into a secure PED as described in section 4.9 of this manual.

Acquirers must control Terminals equipped with PIN pads. If a Terminal is capable of prompting for the PIN, the Acquirer must include the PIN and full magnetic stripe-read data in the Authorization Request/0100 message.

Mastercard will validate the PIN when processing for Issuers that provide the necessary keys to Mastercard pursuant to these Standards. All other POI Transactions containing PIN data will be declined in Stand-In processing.

4.8 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.

4.9 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* manual.
- Each offline-capable Hybrid POS Terminal must support offline Static Data Authentication (SDA) and offline Dynamic Data Authentication (DDA) as Card authentication methods (CAMs). Each offline-capable Hybrid POS Terminal certified by Mastercard on or after 1 January 2011 also must support offline Combined Data Authentication (CDA) as a CAM.
- Except in the United States Region, each offline-capable Hybrid POS Terminal certified by Mastercard on or after 1 January 2011 must support offline PIN processing as a Cardholder Verification Method (CVM). In Taiwan, this requirement applies to Hybrid POS Terminals certified by Mastercard on or after 1 January 2013.
- In the United States Region, each Hybrid POS Terminal that supports PIN must support both online PIN and offline PIN processing.
- Each Hybrid POS Terminal that supports offline PIN processing must support both clear text and encrypted PIN options.

4.10 PIN Entry Device Standards

A PED on an ATM Terminal, Bank Branch Terminal, or POS Terminal must have a numeric keyboard to enable the entry of PINs, with an 'enter key' function to indicate the completion of entry of a variable length PIN.

In all Regions except the Canada and United States Regions, a PED must accept PINs having four to six numeric characters. In the Canada and U.S. Regions, a PED must support PINs of up to 12 alphanumeric characters. It is recommended that all PEDs support the input of PINs in letter-number combinations as follows:

1	Q, Z	6	M, N, O
2	A, B, C	7	P, R, S
3	D, E, F	8	T, U, V
4	G, H, I	9	W, X, Y
5	J, K, L		

An Acquirer must ensure that all PEDs that are part of POS Terminals meet the following Payment Card Industry (PCI) requirements:

1. All PEDs must be compliant with the *Payment Card Industry PIN Security Requirements* manual.
2. All newly installed, replaced, or refurbished PEDs must be compliant with the PCI POS PED Security Requirements and Evaluation Program.
3. All PEDs must be in compliance with the PCI POS PED Security Requirements and Evaluation Program or appear on the Mastercard list of approved devices.

As a requirement for PED testing under the PCI POS PED Security Requirements and Evaluation Program, the PED vendor must complete the forms in the *Payment Card Industry POS PIN Entry Device Security Requirements* manual, along with the *Payment Card Industry POS PIN Entry Device Evaluation Vendor Questionnaire*. The vendor must submit all forms together with the proper paperwork, including the required PED samples, to the evaluation laboratory.

If a Customer or Mastercard questions a PED with respect to physical security attributes (those that deter a physical attack on the device) or logical security attributes (functional capabilities that preclude, among other things, the output of a clear text PIN or a cryptographic key), Mastercard has the right to effect an independent evaluation performed at the manufacturer's expense.

Mastercard will conduct periodic security reviews with selected Acquirers and Merchants. These reviews will ensure compliance with Mastercard security requirements and generally accepted best practices.

WARNING:

The physical security of the PED depends on its penetration characteristics. Virtually any physical barrier may be defeated with sufficient effort.

For secure transmission of the PIN from the PED to the Issuer host system, the PED 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).

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.

4.11 Wireless POS Terminals and Internet/Stand-alone IP-enabled POS Terminal Security Standards

Mastercard has established security requirements for the encryption of sensitive data by POS Terminals. These requirements apply to POS Terminals that use wide area wireless technologies, such as general packet radio service (GPRS) and code division multiple access (CDMA), to communicate to hosts and stand-alone IP-connected terminals that link through the Internet.

All wireless POS Terminals and Internet/IP-enabled POS Terminals must support the encryption of Transaction and Cardholder data between the POS Terminal and the server system with which they communicate, using encryption algorithms approved by Mastercard.

If the deployed Internet/IP-enabled POS Terminals are susceptible to attacks from public networks, Acquirers must ensure that they are approved by the Mastercard IP POS Terminal Security (PTS) Testing Program.

Internet/IP-enabled POS Terminals may be submitted for security evaluation at laboratories recognized by the Mastercard IP PTS Testing Program for subsequent approval.

All Acquirers deploying wireless POS Terminals or Internet/IP-enabled POS Terminals must refer to the following required security documents:

- *POS Terminal Security Program—Program Manual*
- *POS Terminal Security Program—Security Requirements*
- *POS Terminal Security Program—Derived Test Requirements*
- *POS Terminal Security Program—Vendor Questionnaire*
- *Payment Card Industry Data Security Standard* (produced by the PCI Security Standards Council)
- Any other related security documents that Mastercard may publish from time to time.

4.12 POS Terminals Using Electronic Signature Capture Technology (ESCT)

An Acquirer that deploys POS Terminals using Electronic Signature Capture Technology (ESCT) must ensure the following:

- Proper electronic data processing (EDP) controls and security are in place, so that digitized signatures are recreated on a Transaction-specific basis. The Acquirer may recreate the signature captured for a specific Transaction only in response to a retrieval request for the Transaction.
- Appropriate controls exist over employees with authorized access to digitized signatures maintained in the Acquirer or Merchant host computers. Only employees and agents with a "need to know" should be able to access the stored, electronically captured signatures.
- The digitized signatures are not accessed or used in a manner contrary to the Standards.

Mastercard reserves the right to audit Customers to ensure compliance with these requirements and may prohibit the use of ESCT if it identifies inadequate controls.

4.13 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.

4.14 Triple DES Migration 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 PEDs that are part of ATM Terminals must be Triple DES compliant.
- All PIN-based 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**. All Transactions routed to the Interchange System must be Triple DES compliant.

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 Member Information tool, 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.

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 or real-time alerts. Acquirer staff trained to identify potential fraud must analyze the data in these reports within 24 hours.

6.2.2.1 Acquirer Authorization Monitoring Requirements

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

- Number of authorization requests above 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
- Increased number of authorization requests
- Merchant authorization reversals that do not match a previous purchase Transaction
- Out-of-pattern Transaction volume, including but not limited to:
  - Repeated authorization requests
  - High velocity authorizations
  - Technical fallback of chip to magnetic stripe
  - High volume of Contactless Transactions
  - Sequential Account generated attacks
  - Unusual activity in connection with the use of Cards or Accounts issued under a particular BIN

6.2.2.2 Acquirer Merchant Deposit Monitoring Requirements

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

The Acquirer must compare daily deposits against the average Transaction count and amount for each Merchant over a period of at least 90 days, to lessen the effect of normal variances in a Merchant's business. For new Merchants, the Acquirer should compare the average Transaction count and amount for other Merchants within the same MCC assigned to the Merchant. 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.

6.2.2.3 Acquirer Channel Management Requirements

Mastercard requires the Acquirer to monitor, on a regular basis, each parent Member ID/ICA number, child Member ID/ICA number, and individual Merchant 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)

6.2.2.4 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 high-risk Merchants
- PAN key-entry Transactions exceeding ratio
- Abnormal hours (i.e., outside of normal business hours) or seasons
- Inactive Merchants (i.e., those Merchants that have not yet started to accept Cards as well as those that have ceased to accept Cards)
- Transactions with no approval code
- Transaction decline rate
- Inconsistent authorization and clearing data elements for the same Transactions
- Mastercard *SecureCode* authentication rate
- Fraud volume per Merchant
- Any Merchant exceeding the Acquirer's total Merchant average for fraud by 150 percent or more

6.2.2.5 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.

For effective performance, an Acquirer's fraud detection tool should minimally measure the amount and number of fraud Transactions incurred, calculated for each of its Merchants, Payment Facilitators and other Service Providers, and deployed Terminals.

6.2.2.6 Ongoing Merchant Monitoring

An Acquirer must implement procedures for the conduct of periodic ongoing reviews of a Merchant's Card acceptance 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

- 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.

6.3 Mastercard Counterfeit Card Fraud Loss Control Standards

Mastercard actively assists law enforcement in the pursuit of organized and informal criminal groups engaged in counterfeit fraud. Although Mastercard has achieved substantial success in this area, including numerous convictions of counterfeiters and seizures of their physical plants, organized criminal elements continue to expand, with new groups emerging almost daily.

In addition to implementing the fraud loss controls described in section 6.2, Customers must also make a good-faith attempt to limit counterfeit losses. At a minimum, an Issuer is required to incorporate the Card security features described in Chapter 3 on all Cards, and an Acquirer must transmit full magnetic stripe or chip data on all Card-read POS Transactions.

6.3.1 Counterfeit Card Notification

All Customers must notify Mastercard immediately upon suspicion or detection of counterfeit Cards.

6.3.1.2 Notification by Acquirer

An Acquirer detecting or suspecting a counterfeit Card bearing neither a valid BIN nor a valid Member ID immediately must notify its regional Franchise representative and the Issuer by phone, email, or telex communication. Mastercard will add the account number to the Account Management System.

6.3.1.3 Failure to Give Notice

Failure by the Acquirer or Issuer to give notice within 24 hours of detecting a counterfeit Card relieves Mastercard of any responsibility for any resulting loss incurred by any party failing to give notice.

6.3.2 Responsibility for Counterfeit Loss

Certain losses resulting from counterfeit Transactions are the responsibility of either the Issuer or Acquirer based on the circumstances described in this section.

6.3.2.1 Loss from Internal Fraud

Mastercard is not responsible for any loss arising from or related to any fraudulent, dishonest, or otherwise wrongful act of any officer, director, or employee of a Customer, or of a Customer's Service Provider, agent, or representative.

6.3.2.3 Transactions Arising from Unidentified Counterfeit Cards

The Acquirer is responsible for any counterfeit loss resulting from or related to the acceptance by a Merchant of a Card that cannot be identified by the BIN or Member ID imprinted in the Transaction record.

6.3.3 Acquirer Counterfeit Liability Program

The Acquirer Counterfeit Liability Program is intended to combat increases in worldwide counterfeiting in the credit card industry. The Program shifts partial counterfeit loss liability to Acquirers that exceed worldwide counterfeit Standards.

Global Risk Management Program staff uses the Acquirer counterfeit volume ratio (ACVR) to evaluate all Customers' volumes of acquired counterfeit. The ACVR is a Customer's dollar volume of acquired counterfeit as a percentage of the total dollar volume acquired by that Customer.

Global Risk Management Program staff monitors the 20 Customers with the highest ACVRs on a quarterly basis. Mastercard notifies each Customer with liability of its own ACVR, the worldwide average, the reported counterfeit, and the amount of Customer liability calculated on a quarterly basis.

Mastercard uses funds obtained from Acquirers that exceed established annual thresholds to provide the following support:

- Recover the costs associated with the administration of this Program,
- Fund the development of new fraud control programs, and
- Supplement the Mastercard liability limit for the reimbursement of Issuers' counterfeit losses.

6.3.3.1 Acquirer Counterfeit Liability

An Acquirer is liable for any counterfeit volume that is above a threshold of 10 times the worldwide ACVR.

Global Risk Management Program review teams will provide a report to Acquirers whose ACVR exceeds 10 times the worldwide average with recommendations on how to reduce the volume of acquired counterfeit Transactions. If an Acquirer implements all of the programs recommended by Global Risk Management Program staff, or takes necessary action to curb counterfeit, Mastercard will review the actions taken and may adjust the cumulative liability that would otherwise be imposed by the Program.

Counterfeit experience inconsistent with the implementation of the required programs will result in further Customer Risk Reviews by Mastercard.

For more information about the Global Risk Management Program, refer to Chapter 13 of this manual.

6.3.3.2 Acquirer Liability Period

The Acquirer's ACVR liability is computed for the period from 1 January through 31 December. ACVR liability is determined after final submission of counterfeit reimbursement claims for each 12-month cycle.

6.3.3.3 Relief from Liability

To qualify for relief from liability, an Acquirer must meet the following criteria:

1. The Acquirer must comply with the Acquirer loss control program Standards described in section 6.2.2.
2. The Acquirer must issue internal procedures designating responsibilities for monitoring the exception reports, explaining how they should be used, and defining actions to be taken when thresholds are exceeded. Customers will need to maintain internal records that clearly demonstrate supervisory review of such procedures and the periodic review of results by senior management.
3. The Acquirer must transmit the full, unedited ISO 8583 (Financial transaction card originated messages—Interchange message specifications) authorization message from Terminal-read Transactions to the system.
4. The Acquirer that is subject to liability may be required by Mastercard to take additional action to attempt further to reduce its level of counterfeit losses.

Mastercard will provide relief from reversal of responsibility to Acquirers that exceed the threshold under the Acquirer Counterfeit Liability Program and that fully meet the aforementioned criteria.

NOTE: Acquirers must submit a written application for relief in order for Mastercard to provide relief from responsibility.

6.3.3.4 Application for Relief

An Acquirer must submit the written application for relief under signature of an appropriate officer, such as the Card center manager of that Customer. The following information must be included in the application:

- Certification that the requisite controls are in place
- A detailed description of the controls
- The specific parameters being used
- A copy of the procedures document described in section 6.3.3.3
- Sample copies of the automated exception reports

The application for relief must be submitted to the vice president of Franchise at the address provided in Appendix B. Appendix B

The effective date of the provisions of relief will be no sooner than 90 days after the Acquirer has fully implemented the requisite controls. Release from responsibility for the Acquirer will

not be granted until all of the requirements are in place for at least 90 days. Continued eligibility for relief will be subject to periodic review by Franchise staff, and may be revoked at any time.

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

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

7.1 Screening New Merchants, Submerchants, and ATM Owners

A Customer is responsible for verifying that a prospective Merchant, Submerchant, 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 Submerchant, 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 within the Area of Use of the Acquirer's License, as described in Rule 5.4, "Merchant Location", and Rule 5.5, "Submerchant Location", of 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 Submerchant 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 Submerchants of its Payment Facilitators; and
- 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*).

NOTE: A Customer must participate in the MATCH system unless excused by Mastercard or prohibited by law. If a Merchant or Submerchant 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 Submerchant to the MATCH system.

7.1.2 Retention of Investigative Records

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

- Signed Merchant, Submerchant, or ATM Owner Agreement
- With respect to the screening of a Merchant or Submerchant, 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 Submerchant 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 Submerchant is offering the Cardholder for sale
- Date-stamped MATCH inquiry records
- Date-stamped MATCH addition record
- All Customer correspondence with the Merchant, Submerchant, or ATM owner
- All correspondence relating to Issuer, Cardholder, or law enforcement inquiries concerning the Merchant, Submerchant, 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 Provider", 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 Submerchants, in an effort to deter fraud. Monitoring must focus on changes in activity over time, activity inconsistent with the Merchant's or Submerchant'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 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 Submerchant's website(s).

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

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 Submerchants.

7.4 Additional Requirements for Certain Merchant and Submerchant Categories

An Acquirer of a non-face-to-face adult content and services Merchant or Submerchant, non–face-to-face gambling Merchant or Submerchant, non–face-to-face pharmaceutical and tobacco product Merchant or Submerchant, government-owned lottery Merchant or Submerchant, skill games Merchant or Submerchant (U.S. Region only), high-risk cyberlocker Merchant or Submerchant, recreational cannabis Merchant or Submerchant (Canada Region only), and/or Merchant or Submerchant reported under the Excessive Chargeback Program (ECP) must comply with the registration and monitoring requirements of the Mastercard Registration Program (MRP) for each such Merchant or Submerchant, 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 Customer Performance Integrity by sending an email to cpi@mastercard.com.

8.2 Global Merchant Audit Program

The Global Merchant Audit Program (GMAP) uses a rolling six months of data to identify Mastercard Merchant locations that, in any calendar month, meet the criteria set forth in Table 8.1.

Table 8.1—Fraud Criteria for Global Merchant Audit Program Tier Classification

A Mastercard Merchant location is classified in the following GMAP tier...	If in any calendar month, the Mastercard Merchant location meets the following fraud criteria...
Tier 1—Informational Fraud Alert	• Three fraudulent Transactions • At least USD 3,000 in fraudulent Transactions • A fraud-to-sales dollar volume ratio minimum of 3% and not exceeding 4.99%
Tier 2—Suggested Training Fraud Alert	• Four fraudulent Transactions • At least USD 4,000 in fraudulent Transactions • A fraud-to-sales dollar volume ratio minimum of 5% and not exceeding 7.99%
Tier 3—High Fraud Alert	• Five fraudulent Transactions • At least USD 5,000 in fraudulent Transactions • A fraud-to-sales dollar volume ratio minimum of 8%

If a Mastercard Merchant location is identified in multiple tiers during any rolling six-month period, GMAP will use the highest tier for the Merchant identification.

NOTE: If a Mastercard Merchant has more than one location (or outlet), the program criteria apply to each location independently.

8.2.1 Acquirer Responsibilities

Mastercard will notify an Acquirer of the identification of a Tier 1, Tier 2, or Tier 3 Merchant through the Merchant Online Status Tracking (MOST) tool. GMAP Merchant identifications are provided for information only and no Acquirer response is necessary. If Mastercard notifies an Acquirer through MOST that a Tier 3 special Merchant audit has been initiated, the Acquirer must respond as described in section 8.2.2.

When a Merchant is identified in Tier 1, Tier 2, or Tier 3, the Acquirer should evaluate the fraud control measures and Merchant training procedures in place for the Merchant. Mastercard strongly recommends that the Acquirer act promptly to correct any identified deficiencies. Suggested enhancements are described in the *GMAP Best Practices Guide for Acquirers and Merchants to Control Fraud*.

Mastercard, in its sole discretion, may conduct an audit to determine whether a Merchant location is in violation of the Valid Transactions Rule, as described in section 5.12 of the *Mastercard Rules*, and may assign chargeback liability.

8.2.2 Tier 3 Special Merchant Audit

If GMAP identifies a Merchant location in Tier 3, Mastercard will determine whether to initiate an audit of the Merchant location ("a Tier 3 special Merchant audit"). If Mastercard decides to conduct a Tier 3 special Merchant audit, the audit will proceed as follows:

1. **Mastercard notifies Acquirer.** The Acquirer will receive notification from Mastercard, through MOST, that a Tier 3 special Merchant audit has been initiated.
2. **Acquirer response due within 30-day response period.** No later than 30 days after the Tier 3 special Merchant audit notification date ("the 30-day response period"), the Acquirer must respond to the audit notification through MOST by either:

   a. Notifying Mastercard that the Acquirer has terminated the Merchant (if the Acquirer determines that the Merchant must be reported to the Mastercard Alert to Control High-risk [Merchants] [MATCH™] system, the Acquirer may do so through MOST), or;
   b. Completing the online questionnaire, if the Acquirer did not terminate the Merchant. This questionnaire is used to inform Mastercard of 1) any exceptional or extenuating circumstances pertaining to the identified Merchant's fraud and 2) the fraud control measures in place at the Merchant location.

   Upon review of the completed online questionnaire, Mastercard, at its sole discretion, may:

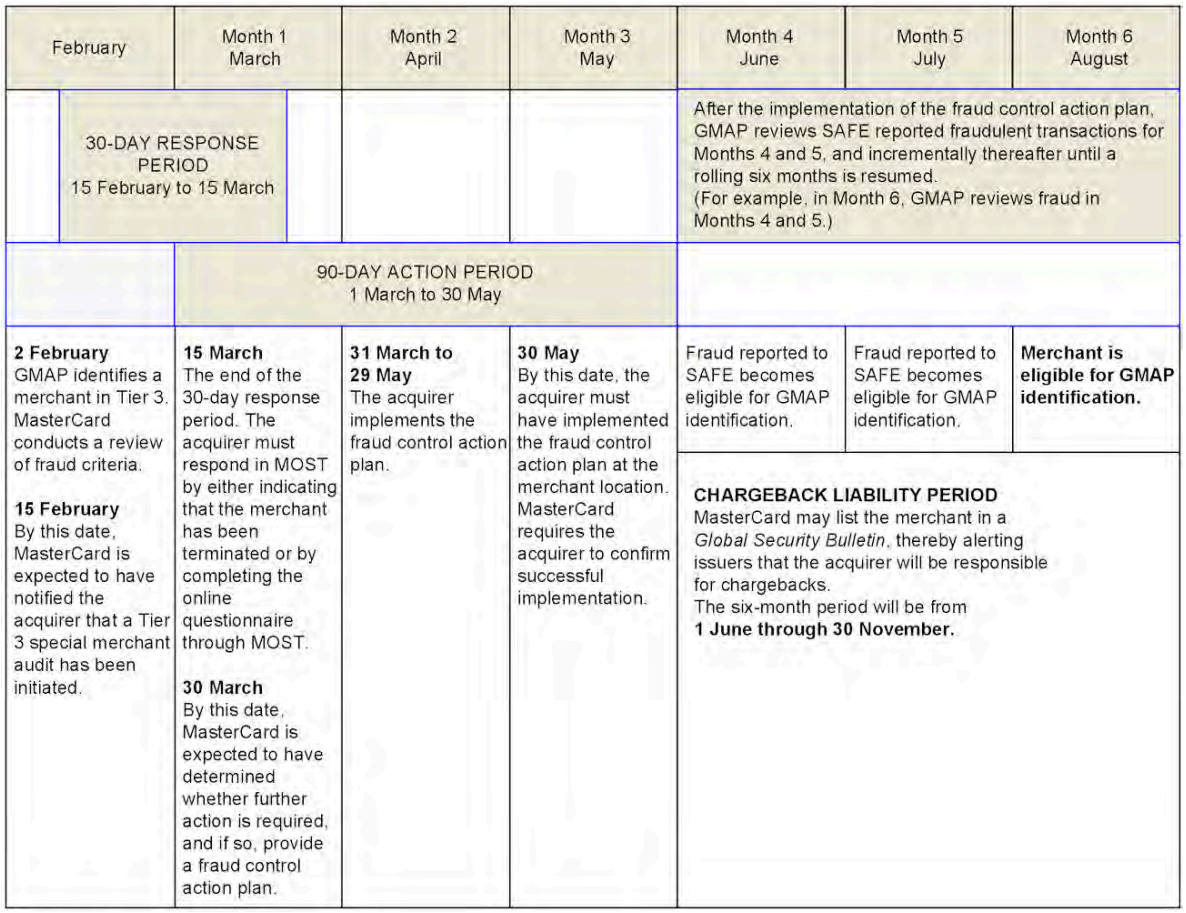
   – Grant the Merchant location an exclusion for the Merchant identification, or;
   – Provide the Acquirer with the opportunity to implement additional fraud control measures ("the fraud control action plan"), as directed by Mastercard, at the Merchant location, or;
   – Assign chargeback responsibility to the Acquirer for the Merchant location.

3. **Fraud control action plan required within 90-day action period.** If Mastercard requires the Acquirer to implement a fraud control action plan, Mastercard will provide the plan to the Acquirer through MOST. The Acquirer has 90 days from the first day of the month following the month in which the Merchant was identified in GMAP ("the 90-day action period") to take all required actions, including but not limited to confirmation that such fraud control action plan has taken effect. Mastercard may extend the 90-day action period at its sole discretion. For Acquirers that implement a fraud control action plan, the identified Merchant is again eligible to be newly identified in GMAP commencing on the sixth month following the month in which the Merchant was first identified in GMAP. Fraudulent Transactions reported to the System to Avoid Fraud Effectively (SAFE) will be reviewed under the Program commencing on the fourth and fifth months following the month in which the Merchant was first identified in GMAP, and will continue incrementally thereafter until the Merchant resumes a six-month rolling review period, provided the Merchant does not exceed the GMAP Tier 1, 2, or 3 thresholds.

The Acquirer of a Merchant subject to a Tier 3 special Merchant audit must provide satisfactory documentation to substantiate that reasonable controls to combat fraud have been implemented, including implementation of a Mastercard directed fraud control action plan.

Refer to Figure 8.1 for a sample timeline of a Tier 3 special Merchant audit.

Figure 8.1—Tier 3 Special Merchant Audit Sample Timeline



8.2.3 Chargeback Responsibility

Mastercard will review each Acquirer of a Merchant location subject to a Tier 3 special Merchant audit on a case-by-case basis and determine, at the sole discretion of Mastercard, if a chargeback liability period is applicable. The chargeback liability period is for six months and begins on the first day of the fourth month following the GMAP Tier 3 identification.

Mastercard, at its sole discretion, may extend the chargeback liability period to 12 months.

Mastercard reserves the right to list the Acquirer ID, Acquirer name, Merchant name, Merchant location, and chargeback liability period of any Tier 3 Merchant in a Mastercard Announcement (AN) available on the Technical Resource Center on Mastercard Connect™.

When Mastercard lists the Acquirer and Merchant information in a Mastercard Announcement, Issuer chargeback rights will apply. Each Issuer then has a right to use message reason code 4849—Questionable Merchant Activity to charge back to the Acquirer any fraudulent Transactions from the Merchant that are reported to SAFE with the following fraud types:

- 00—Lost Fraud,

- 01—Stolen Fraud,
- 04—Counterfeit Card Fraud,
- 06—Card Not Present Fraud, or
- 07—Multiple Imprint Fraud.

Each Transaction charged back must have occurred during the published chargeback period and must be reported to SAFE within the applicable time frame (refer to Chapter 12 of this manual). Issuers may not use message reason code 4849 to charge back Transactions from an Acquirer and Merchant identified in GMAP if the fraud type is:

- 02—Never Received Issue,
- 03—Fraudulent Application,
- 05—Account Takeover Fraud, or
- 51—Bust-out Collusive Merchant.

Once Mastercard lists the Acquirer ID, Acquirer name, Merchant name, Merchant location, and chargeback responsibility period in a Mastercard Announcement, the Issuer may not use message reason code 4849—Questionable Merchant Activity, in any of the following situations:

- The Transaction was not reported properly to SAFE within the applicable time frame specified in this manual.
- The Transaction was reported to SAFE as a fraud type of Never Received Issue (02), Fraudulent Application (03), Account Takeover Fraud (05), or Bust-out Collusive Merchant (51).
- If the *SecureCode* and Mastercard Identity Check global liability shift for electronic commerce (e-commerce) Transactions is in effect, and all of the following conditions occur:
  - The Merchant is Universal Cardholder Authentication Field (UCAF™)-enabled, and
  - The Issuer provided the Accountholder Authentication Value (AAV) from the Mastercard Secure Payment Application (SPA) algorithm, and
  - All other e-commerce Authorization Request/0100 message and clearing requirements were satisfied, and
  - The Authorization Request Response/0110 message reflected the Issuer's approval of the Transaction.
- If an intracountry or intraregional chip liability shift or the interregional Chip Liability Shift Program (Level 1) is in effect, the Transaction was processed at a chip compliant Terminal, the Transaction was reported to SAFE as counterfeit fraud, and either the Transaction was identified properly as 1) an offline Chip Transaction in the clearing record, or 2) as an online Transaction in the Authorization Request/0100 message, and the Authorization Request Response/0110 message reflected the Issuer's approval of the Transaction.

8.2.4 Exclusion from the Global Merchant Audit Program

The following sections address exclusions from GMAP.

[1] Refer to Issuer restrictions on chargebacks for message reason code 4849 for the Mastercard® *SecureCode*™ global liability shift as described later in this section.

8.2.4.1 Systematic Exclusions

The following Transactions systematically are excluded for the purposes of determining the identification of a Merchant in GMAP:

- **Debit Fraud**—This includes all fraud related to Cirrus (CIR) and Maestro (MSI).
- **All Never Received Issue, Fraudulent Application, Account Takeover (ATO), and Bust-out Collusive Merchant fraud types**—This includes all Transactions reported to SAFE as fraud type:
  - 02—Never Received Issue
  - 03—Fraudulent Application
  - 05—Account Takeover Fraud
  - 51—Bust-out Collusive Merchant

8.2.4.2 Exclusion After GMAP Identification

After Mastercard provides notification to an Acquirer that a Tier 3 special Merchant audit has been initiated, the Acquirer may request that Mastercard exclude the Merchant for good cause.

When requesting an exclusion, the Acquirer must submit the completed special Merchant audit online questionnaire within 30 days of the Tier 3 special Merchant audit notification and provide such other supporting information that Mastercard requires.

Mastercard staff will decide whether to exclude a Merchant from GMAP.

When evaluating exclusion requests, Mastercard may consider such matters as:

- **A fraud-to-sales dollar volume ratio below 8 percent**—If the Merchant's Mastercard dollar volume is not systematically available for calculation, the Acquirer will have the opportunity to provide this data to Mastercard for review. To recalculate the Merchant fraud-to-sales dollar volume ratio, the Acquirer must present supporting documentation to show only the Mastercard sales for the identified location during the applicable months in which the identification criteria are met.

  If the supporting documentation demonstrates that the Merchant location did not exceed the Tier 3 fraud thresholds, the Acquirer will receive an exclusion for the Merchant.

  If the supporting documentation demonstrates that the Merchant's fraud-to-sales ratio exceeds 8 percent, Mastercard will take action as described in section 8.2.2.
- **The fraud control Program currently in place at the Merchant location**—Mastercard will review information pertaining to the fraud control Program currently in place at the Merchant location to establish if additional fraud control measures could have prevented or reduced the fraud.
- **A chain Merchant**—A chain Merchant is defined in the *IPM Clearing Formats* under Data Element (DE) 43 (Card Acceptor Name/Location) as one of multiple Merchant outlets having common ownership and selling the same line of goods or services. Mastercard Standards further indicate that subfield 1 (Card Acceptor Name) of this data element must contain a unique identifier at the end of this field if the Merchant has more than one location in the same city. It is the Acquirer's responsibility to ensure that all Merchants of

this nature are identified properly. Merchants with multiple locations that are in compliance with this Standard are identified uniquely in the audit programs.

Acquirers with a Merchant subject to a Tier 3 special Merchant audit based on a calculation inclusive of more than one location may apply for an exclusion. To apply for such an exclusion, the Acquirer must provide Mastercard with fraud and sales data for each location within the chain. If the same Merchant ID number is used to identify all of the Merchant locations, the Acquirer must further provide a copy of the sales draft for each Transaction identified as fraudulent.

Exclusions based on other exceptional or extenuating circumstances—An Acquirer may request an exclusion for a Merchant location from a Tier 3 special Merchant audit based on exceptional or extenuating circumstances by providing appropriate information.

The following are examples of information that Mastercard will consider with regard to an exclusion request for exceptional or extenuating circumstances:

1. SAFE data error:
   - Erroneous Transaction amount reported
   - Reported Transaction amount inflated as a result of currency conversion
   - Transaction reported under incorrect Acquirer ID or Merchant name
   - Duplicate Transactions reported
   - Non-fraudulent Transaction reported to SAFE in error (such as a dispute)
2. The Merchant captured fraudulent Card(s) transacted at its location.
3. The Merchant assisted with the apprehension and conviction of criminal(s) that transacted fraudulent Cards at its location.
4. The Merchant identified fraudulent Transactions before shipping merchandise and issued credits to the Cardholder account in a timely fashion, provided the credit was not issued in response to a retrieval request or chargeback.

8.2.5 Notification of Merchant Identification

When a Merchant location is identified in GMAP, Mastercard will report the Merchant identification in MOST, detailing the identification.

In addition, the Acquirer will receive the Global Merchant Audit Program Report.

Acquirers must use MOST to respond to a Tier 3 special Merchant audit notification.

NOTE: Acquirers are responsible for ensuring that they are capable of receiving notification of Merchants identified in GMAP. If an Acquirer does not receive an automated notification, it is the Acquirer's responsibility to obtain this information through Mastercard Connect™.

8.2.5.1 Distribution of Reports

Refer to the *MOST Users' Manual* for information about the distribution of GMAP reports.

8.2.6 Merchant Online Status Tracking (MOST) System

The MOST system resides on the Mastercard Connect platform, and is used to administer the process for Merchants identified in GMAP. The MOST system allows an Acquirer to:

- View each Merchant identified in GMAP
- Determine the reasons that a Merchant was identified in GMAP
- Retrieve full Transaction details for each identified Merchant from Fraud Reporter
- View the status of each Merchant subject to a Tier 3 special Merchant audit
- Complete an online questionnaire as required by Mastercard for a Tier 3 special Merchant audit
- Determine the chargeback liability period for each Merchant subject to a Tier 3 special Merchant audit

8.2.6.1 MOST Mandate

Acquirers must use the MOST system available on Mastercard Connect when required by Mastercard to respond to a Tier 3 special Merchant audit in MOST. Mastercard will assess a USD 100 processing fee per individual Merchant identification for an Acquirer that does not solely use MOST to respond to a Tier 3 special Merchant audit.

Mastercard will assess the USD 100 processing fee only one time for each required Tier 3 special Merchant audit response. The fee will be collected by debiting the Acquirer's Mastercard Consolidated Billing System (MCBS) account.

In addition, Mastercard may assess an Acquirer a USD 100 processing fee if the Tier 3 special Merchant audit response is completed in MOST and is submitted using any other additional method. However, if an Acquirer responds to a Tier 3 special Merchant audit through MOST and then chooses to submit supporting documentation through another communication method, or to engage in dialogue with Mastercard staff, then Mastercard will not assess the Acquirer a processing fee.

MOST and MATCH have been incorporated into one suite of mandated products for which Acquirers globally are assessed a combined annual fee of USD 5,000.

8.2.6.2 MOST Registration

To use MOST, a user must be licensed for each acquiring Customer/ICA number at a child level, regardless of a parent/child relationship. To request access to MOST, a user signs in to Mastercard Connect with his or her User ID and password, then orders MOST for specific Customers/ICA numbers from the Mastercard Connect Store.

The order then is routed to the user's Security Administrator for approval. If a different company owns the Customer/ICA number data, then the order is routed to the Security Administrator of the company that owns the data. The Security Administrator is responsible for approving the user's order for MOST. After the appropriate Security Administrators approve the order, it is routed to Mastercard for processing. The user has access to MOST after Mastercard approves the order. Users must have an RSA SecurID® to use MOST. If the user does not have a SecurID, one will be issued as part of the access approval process.

Mastercard will decline orders for MOST that are not complete and accurate. Mastercard reserves the right to request written authorization from a Customer's Security Contact, Principal Contact, or MATCH Contact to validate the user's request for MOST. If Mastercard declines an order, the user must submit a subsequent order for MOST through the Mastercard Connect Store.

For additional assistance with ordering MOST, contact the Global Customer Service team using the information provided in section B.6 of Appendix B.

8.3 Excessive Chargeback Program

Mastercard designed the Excessive Chargeback Program (ECP) to encourage each Acquirer to closely monitor, on an ongoing basis, its chargeback performance at the Merchant level and to determine promptly when a Mastercard Merchant has exceeded or is likely to exceed monthly chargeback thresholds.

8.3.1 ECP Definitions

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

Merchant

A Merchant is defined as any distinct Mastercard Merchant location, whether a Merchant's physical location or a Merchant's Internet site or uniform resource locator (URL) that is identified by a distinct billing descriptor by the Acquirer in the Transaction record.

Chargeback-to-Transaction Ratio (CTR)

The CTR is the number of Mastercard chargebacks received by the Acquirer for a Merchant in a calendar month divided by the number of the Merchant's Mastercard sales Transactions in the preceding month acquired by that Acquirer. (A CTR of 1% equals 100 basis points, and a CTR of 1.5% equals 150 basis points.)

Chargeback-Monitored Merchant (CMM)

A CMM is a Merchant that has a CTR in excess of 100 basis points and at least 100 chargebacks in a calendar month.

Excessive Chargeback Merchant (ECM)

A Merchant is an ECM if in each of two consecutive calendar months (the "trigger months"), the Merchant has a minimum CTR of 150 basis points and at least 100 chargebacks in each month. This designation is maintained until the ECM's CTR is below 150 basis points for two consecutive months.

Tier 1 ECM

A Merchant is a Tier 1 ECM during the first through sixth month (whether consecutive or non-consecutive) that the Merchant is identified as an ECM.

Tier 2 ECM

A Merchant is a Tier 2 ECM during the seventh through twelfth month (whether consecutive or non-consecutive) that the Merchant is identified as an ECM.

8.3.2 Reporting Requirements

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.

The ECP requires an Acquirer to calculate, for each calendar month, the CTR in basis points for each of its Merchants and report to Mastercard any Merchant that is a CMM or ECM as defined in section 8.3.1.

Mastercard will assess an Acquirer of an ECM the reporting fee set forth in section 8.3.2.2.

8.3.2.1 Chargeback-Monitored Merchant Reporting Requirements

Each calendar month, an Acquirer must submit to Mastercard a separate CMM report for each of its Merchant(s) that qualifies as a CMM for the previous calendar month. For the purpose of determining if an Acquirer is obligated to submit a CMM report, the Acquirer must calculate the CTR as set forth in section 8.3.1. The Acquirer must submit this report no later than 45 days from the end of the calendar month.

The Acquirer must submit the CMM report in a form and manner required by Mastercard. The Acquirer also must provide a copy of the CMM report and these ECP Standards to the specific CMM.

The Acquirer must continue to provide CMM reporting until the Merchant is no longer identified as a CMM for two consecutive months.

8.3.2.1.1 CMM Report Contents

The CMM report must include all of the following information:

- The name and location of the CMM
- The calendar month of CMM qualification being reported
- The CTR of the CMM for the reported calendar month
- The Card acceptor business code/Merchant category code (MCC) assigned to the CMM and a description of the nature of the CMM's business
- The number and gross dollar volume (GDV) of the CMM's Mastercard sales Transactions in the reported calendar month and in the preceding month
- The number and GDV of chargebacks of the CMM's Mastercard sales Transactions for the reported calendar month
- Any additional information as Mastercard may require

8.3.2.1.2 Late CMM Report Submission Assessment

If Mastercard determines that a Merchant is a CMM and the Acquirer fails to submit a timely CMM report to Mastercard for that Merchant, Mastercard may assess the Acquirer up to USD 5,000 per month for each month that a specific monthly CMM report is overdue.

8.3.2.2 Excessive Chargeback Merchant Reporting Requirements

Within 30 days of the end of the second trigger month, and on a monthly basis thereafter, the Acquirer must submit a separate ECM report for each of its ECMs (in lieu of a CMM report)

until that ECM's CTR is below 150 basis points for two consecutive months. The Acquirer also must provide a copy of the ECM report and these ECP Standards to the specific ECM. Mastercard will assess the Acquirer a reporting fee of USD 100 for each ECM report submitted.

The Acquirer must continue to provide monthly ECM reporting until the Merchant is no longer identified as an ECM for two consecutive months. If during those months the Merchant is identified as a CMM, then the CMM reporting requirements will apply.

8.3.2.2.1 ECM Report Contents

The ECM report must include all of the information required for the CMM report, and the following additional information:

- A completed Mastercard Excessive Chargeback Program (ECP)—Action Plan (Form 1288)
- An electronic file that contains chargeback Transaction details for each chargeback received by the Acquirer for the ECM in the calendar month
- Any additional information as Mastercard may require from time to time

The Mastercard ECP—Action Plan is available on the Forms page of Mastercard Connect™.

Mastercard will assess the Acquirer a reporting fee of USD 100 for each ECM report submitted.

8.3.2.2.2 Late ECM Report Submission Assessment

If Mastercard determines that a Merchant is an ECM and the Acquirer fails to submit a timely ECM report to Mastercard for that ECM, Mastercard may assess the Acquirer up to USD 500 per day for each of the first 15 days that the ECM report for that ECM is overdue and up to USD 1,000 a day thereafter until the delinquent ECM report is submitted.

8.3.3 Assessments

In addition to any applicable assessments for ECM reports or late report submissions, Mastercard may assess the Acquirer for Issuer reimbursement fees and violation assessments for excessive chargebacks arising from an ECM. Mastercard calculates the Issuer reimbursement fees and assessments as described in section 8.3.3.1 and they apply in each calendar month that the ECM exceeds a CTR of 150 basis points after the first trigger month. For the purposes of calculating Issuer reimbursement fees and assessments only (and not for the purpose of satisfying the reporting requirements contained herein), an Acquirer may offer an alternative CTR calculation that more accurately "maps back" or links the chargebacks to the relevant sales Transactions.

For the first 12 months of a Merchant's identification as an ECM, Mastercard will consider the Merchant's actual chargeback volume as a factor in its determination of Acquirer liability. During this period, Mastercard will assess the Acquirer the lesser of:

- The total of the Issuer reimbursement plus violation assessment amounts, calculated as described in section 8.3.3.1 for a given month, or
- The Merchant's chargeback dollar volume reported by the Acquirer for that month.

8.3.3.1 ECP Assessment Calculation

Mastercard determines an Acquirer's liability for the monthly Issuer reimbursement fees and assessments for each ECM as set forth below. Mastercard calculates the Issuer reimbursement fees in the following Steps 1, 2, and 3, and calculates the violation assessment in Step 4.

1. Calculate the CTR for each calendar month that the ECM exceeded a CTR of 150 basis points (which may also be expressed as 1.5% or 0.015).
2. From the total number of chargebacks in the above CTR calculation, subtract the number of chargebacks that account for the first 150 basis points of the CTR. (This amount is equivalent to 1.5 percent of the number of monthly sales Transactions used to calculate the CTR.) The result is the number of chargebacks above the threshold of 150 basis points.
3. Multiply the result from Step 2 by USD 25. This is the Issuer reimbursement.
4. Adjust the result in Step 3 to reflect the extent that the Acquirer has exceeded the 150 basis points threshold by multiplying the value in Step 3 by the CTR (expressed as basis points). Divide this result by 100. This amount is the violation assessment.

Repeat Steps 1–4 for each calendar month (other than the first trigger month) that the ECM exceeded a CTR of 150 basis points or 1.5 percent.

Example: The Acquirer for Merchant ABC acquired Mastercard sales Transactions and chargebacks over a six-month period as follows:

Month	January	February	March	April	May	June	July
Sales Transactions	95,665	95,460	95,561	95,867	95,255	95,889	95,758
Chargebacks	1,050	1,467	1,635	1,556	1,495	1,052	985
CTR in basis points	—	153	171	163	156	110	103

February and March are the trigger months, as these are two consecutive months where the CTR exceeded 150 basis points. At the end of July, Merchant ABC was no longer an ECM as its CTR was below 150 basis points for two consecutive months. Mastercard calculates assessments and Issuer reimbursements for each of the months March through July.

For example, the assessment for April (using March sales Transactions and April chargeback volumes) is calculated as follows:

- The CTR = April chargebacks/March sales Transactions = 1,556/95,561 = 0.01628 or 163 basis points (rounded)
- The number of chargebacks in excess of the 150 basis points is determined by subtracting 1.5 percent of the March sales Transactions from the number of April chargebacks. 1.5 percent of the March sales Transactions (95,561 x 0.015) is 1,433. 1,556 – 1,433 = 123 chargebacks

- The Issuer reimbursement for April is 123 x USD 25 = USD 3,075
- The violation assessment is (USD 3,075 x 163)/100 or 501,225/100 = USD 5,012.25

Using this methodology, the Issuer reimbursement fees and assessments for the Acquirer for Merchant ABC are as follows.

Month	Issuer Reimbursement	Assessment	Total
February (first trigger month)	0	0	0
March (second trigger month)	USD 5,075.00	USD 8,678.25	USD 13,753.25
April	USD 3,075.00	USD 5,012.25	USD 8,087.25
May	USD 1,425.00	USD 2,223.00	USD 3,648.00
June	0	0	0
July	0	0	0
Total	USD 9,575.00	USD 15,913.50	USD 25,488.50

Example: For the month of March, the Acquirer reported Merchant ABC chargeback volume of 1,635 chargebacks totaling USD 12,145. This amount is less than the calculated amount of the Issuer reimbursement plus violation assessment total of USD 13,753.25, as shown above for March. Therefore, Mastercard will assess the Acquirer the lesser chargeback volume amount rather than the greater calculated amount.

8.3.5 Additional Tier 2 ECM Requirements

After a Merchant has been a Tier 1 ECM for six months (whether consecutive or non-consecutive), the Merchant will be deemed a Tier 2 ECM in its seventh month as an ECM.

With respect to a Tier 2 ECM, Mastercard may:

1. Advise the Acquirer with regard to the completed Mastercard ECP—Action Plan (Form 1288) and other measures that the Acquirer should take or consider taking to reduce the Merchant's CTR; and/or
2. Require the Acquirer to undergo a Global Risk Management Program Customer Risk Review, at the Acquirer's expense, as described in Chapter 13 of this manual.

After a Merchant has been an ECM for 12 months (whether consecutive or non-consecutive), the Acquirer will be deemed to be in violation of Rule 5.11.7 of the *Mastercard Rules* manual ("the Illegal or Brand-damaging Transactions Rule"), and in addition to the assessments

described in section 8.3.3, is subject to noncompliance assessments of up to USD 50,000 per month after the twelfth month that the Merchant remains an ECM.

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 resulting from fraudulent Transactions at a Questionable Merchant, based on SAFE 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 government-issued 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).

If an Issuer has reason to believe that a Merchant may be a Questionable Merchant, the Issuer must promptly notify Mastercard by email message at qmap@mastercard.com. 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.

8.4.4 Mastercard Notification to Acquirers

Following the Mastercard evaluation of Transactions reported to SAFE 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 Member Information—Mastercard 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 Member Information—Mastercard 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 SAFE, 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 SAFE as described in section 8.4.3 of this manual, or
4. 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.

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.

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 Mastercard Registration Program Overview

Mastercard requires Customers to register the following Merchant types, including Submerchants, and other entities using the Mastercard Registration Program (MRP) system, available through Mastercard Connect™:

- Non-face-to-face adult content and services Merchants—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 to high_risk_merchant@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 to high_risk_merchant@mastercard.com.
- Government-owned lottery Merchants (specific countries)—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, the Customer must submit the required registration items as described in section 9.4.5 to Mastercard by sending an email to high_risk_merchant@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)
- Merchants reported under the Excessive Chargeback Program (refer to section 8.3)

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, Submerchant, 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, Submerchant, 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, Submerchant, 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 to high_risk_merchant@mastercard.com.

For requirements specific to Merchants that are required to implement the Mastercard Site Data Protection (SDP) Program, refer to section 10.3 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 Submerchant under the categories listed in section 9.1, except Merchants reported under the Excessive Chargeback Program (ECP). 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 Submerchant 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 Submerchant, 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 Submerchant 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, high-risk cyberlocker Transactions, recreational cannabis Transactions (Canada Region only), or Transactions from Merchants reported under the ECP:

- 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 and maintains a total chargeback-to-interchange sales volume ratio below the ECP thresholds. For information about the ECP, refer to section 8.3 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; 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 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 Submerchant, it must register the Merchant with Mastercard as described in section 9.2 of this manual.

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 reflecting non–face-to-face gambling, an Acquirer first must register the Merchant, Submerchant, 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, Submerchant, 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, Submerchant, 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, Submerchant, or other entity with MCC 7801 and TCC U.

In addition to the requirement to register the Merchant, Submerchant, or other entity as described in section 9.2, an Acquirer registering a U.S. Region Merchant, Submerchant, 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 high_risk_merchant@mastercard.com as part of the registration process (herein, all references to a Merchant also apply to a Submerchant 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 in its sole discretion.

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. The Acquirer must also specifically reaffirm its indemnification to Mastercard in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 2.3 of the *Mastercard Rules* manual, regardless of the Acquirer's compliance with the Mastercard *Internet Gambling Policy* or these requirements.

Mastercard must approve the registration request before the Acquirer may process any non-face-to-face gambling Transactions for the U.S. Region Merchant, Submerchant, 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 Submerchant in accordance with this section, the Acquirer of such Merchant or Submerchant must have verified that the Merchant's or Submerchant's activity complies fully with all laws applicable to Mastercard, the Merchant or Submerchant, the Issuer, the Acquirer, and any prospective customer of the Merchant or Submerchant. 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 Submerchant 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 Submerchant 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 Submerchant. 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 Brazil, Norway, Poland, Sweden, and in the Canada Region (see section 9.4.4.2), respectively.

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

A U.S. Region Acquirer must:

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

To register a Merchant, Submerchant, 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 high_risk_merchant@mastercard.com as part of the registration process (herein, all references to a Merchant also apply to a Submerchant 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 in its sole discretion.
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. The Acquirer must also specifically reaffirm its indemnification to Mastercard in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 2.3 of the *Mastercard Rules* manual, regardless of the Acquirer's compliance with Mastercard rules, policies, and procedures or these requirements.

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

9.4.4.2 Government-owned Lottery Merchants (Specific Countries)

A Customer located in Brazil, Norway, Poland, Sweden, or the Canada Region may use MCC 9406 (Government Owned Lottery [Specific Countries]) to identify a Merchant, Submerchant, or other entity 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, Submerchant, 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, Submerchant, or other entity conducting skill games; or
  - A Merchant, Submerchant, 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, Submerchant, or other entity;

  AND
- Must register the Merchant, Submerchant, or other entity with Mastercard as described in section 9.2 and this section 9.4.5.

To register a Merchant, Submerchant, 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 high_risk_merchant@mastercard.com as part of the registration process (herein, all references to a Merchant also apply to a Submerchant 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 in its sole discretion.

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. The Acquirer must also specifically reaffirm its indemnification to Mastercard in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 2.3 of the *Mastercard Rules* manual, regardless of the Acquirer's compliance with Mastercard rules, policies, and procedures or these requirements.

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

9.4.6 High-Risk Cyberlocker Merchants

A non–face-to-face high-risk cyberlocker Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase access directly from a Merchant or Submerchant, 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 high-risk cyberlocker Transactions from a Merchant or Submerchant, it must register the Merchant or Submerchant, as well as any entities that can provide access to such Merchant's or Submerchant's contents and services, with Mastercard as described in section 9.2 of this manual.

In addition, before an Acquirer may process non–face-to-face high-risk cyberlocker Transactions from an entity that can provide access to or accept payments on behalf of a cyberlocker Merchant's or Submerchant's contents and services, it must register the entity, as well as any cyberlocker Merchants for which it provides access, with Mastercard as described in section 9.2 of this manual.

Any cyberlocker Merchant, Submerchant, or entity that provides access to or accepts payments on behalf of such Merchant's or Submerchant's contents and services that meets one or more of the following criteria must be registered by the Acquirer as a high-risk cyberlocker Merchant, and Mastercard will determine, in its sole discretion, if the Merchant, Submerchant, or entity is a high-risk cyberlocker Merchant:

- 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 high-risk cyberlocker Transactions using MCC 4816 (Computer Network/Information Services) and TCC T.

At the time of registration of a Merchant, Submerchant, or entity in accordance with this section, the Acquirer of such Merchant, Submerchant, or entity must have verified that the Merchant's, Submerchant's, or entity's activity complies fully with all laws applicable to Mastercard, the Merchant, Submerchant, entity, the Issuer, the Acquirer, and any prospective customer of the Merchant, Submerchant, 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, Submerchant, 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, Submerchant, 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, Submerchant, 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 Submerchant located in the Canada Region, an Acquirer first must register the Merchant or Submerchant 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 Submerchant whose primary business is the sale of recreational cannabis (For a Canada Region Merchant or Submerchant whose primary business is not the sale of recreational cannabis, the MCC of the Merchant's or Submerchant's primary business must be used); and
- Obtain and retain from the Merchant or Submerchant or a Canadian provincial licensing authority a copy of the provincial retail license permitting the Merchant or Submerchant 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 Submerchant'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 Submerchant loses its licensed status, the Acquirer must stop the Merchant or Submerchant from accepting Mastercard-branded

payments products for recreational cannabis sales and promptly advise Mastercard in writing of such action.

Chapter 10 Account Data Protection Standards and Programs

This chapter may be of particular interest to Customer personnel responsible for protecting Account, Cardholder, and Transaction data; and to Customers that have experienced or wish to protect themselves against Account data compromise events.

10.1 Account Data Protection 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 that store, process, or transmit Card, Cardholder, or Transaction data and all Customer agents that store, process, or transmit Card, Cardholder, or Transaction data on the Customer's behalf adhere to the most current Payment Card Industry PIN Transaction Security Program (PCI PTS) and *Payment Card Industry Data Security Standard* (PCI DSS). The PCI Security Standards are available on the PCI SSC website at http://www.pcisecuritystandards.org.

10.2 Account Data Compromise Events

NOTE: This section 10.2 applies to Mastercard and Maestro Transactions, unless otherwise indicated.

Definitions

As used in this section 10.2, 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, 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), and Data Storage Entities (DSEs) (regardless of whether the TPP or DSE 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 section 10.2, 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 section 10.2, 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 Card Authentication Data

This term has the meaning set forth in the *Payment Card Industry Data Security Standard*, 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 section 10.2 (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 section 10.2, 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.

10.2.1 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 Protection Standards and Programs set forth in this Chapter 10 should request advice from Mastercard Fraud Investigations.

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 10.2 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.

10.2.2 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 under this section 10.2 or to respond fully and in a timely fashion to a request for information to which Mastercard is entitled under this section 10.2, 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.

10.2.2.1 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 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;
    2. isolate compromised systems and media from the network;
    3. preserve all Intrusion Detection Systems, Intrusion Prevention System logs, all firewall, Web, database, and events logs;
    4. document all incident response actions; 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.
- 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 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 not have provided the last PCI compliance report concerning the system or environment to be examined. 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 twenty (20) business days from the commencement of the forensic 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.

10.2.2.2 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.

10.2.3 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 final forensic report required under section 10.2.2.1 must include the following, unless otherwise directed in writing by Mastercard:

- A statement of the scope of the forensic investigation, including sources of evidence and information used by the PFI.
- A network diagram, including all systems and network components within the scope of the forensic investigation. As part of this analysis, all system hardware and software versions, including POS applications and versions of applications, and hardware used by the compromised entity within the past twelve (12) months, must be identified.
- A payment Card Transaction flow depicting all Points of Interaction (POIs) associated with the transmission, processing, and storage of Account data and network diagrams.
- A written analysis explaining the method(s) used to breach the subject entity's network or environment as well as method(s) used to access and exfiltrate Account data.
- A written analysis explaining how the security breach was contained and the steps (and relevant dates of the steps) taken to ensure that Account data are no longer at risk of compromise.
- An explanation of investigative methodology as well as identification of forensic data sources used to determine final report findings.
- A determination and characterization of Account data at-risk of compromise, including the number of Accounts and at-risk data elements.
- The location and number of Accounts where restricted Account data, whether encrypted or unencrypted, was or may have been stored by the entity that was the subject of the forensic investigation. This includes restricted Account data that was or may have been stored in unallocated disk space, backup media, and malicious software output files.

- A time frame for Transactions involving Accounts determined to be at risk of compromise. If the Transaction date/time is not able to be determined, file-creation timestamps must be supplied.
- A determination of whether and, if so, how payment card data was wrongfully disclosed or taken.
- On a requirement-by-requirement basis, a conclusion as to whether, at the time that the ADC Event or Potential ADC Event occurred, each applicable PCI SSC requirement was complied with. For the avoidance of doubt, as of the date of the publication of these Standards, the PCI Security Standards include the PCI DSS, PIN Entry Device (PCI PED) Security Requirements, and *Payment Application Data Security Standard* (PA-DSS).

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 through Secure Upload.

10.2.4 Alternative Standards Applicable to Certain Merchants or Other Agents

In the event of an ADC Event or Potential ADC Event (for purposes of this section 10.2.4, an "Event") for which the subject is a Level 2, Level 3, or Level 4 Merchant (as set forth in section 10.3.4), in lieu of complying with the responsible Customer obligations set forth in section 10.2.2.1, the first bullet point of section 10.2.2.2, and section 10.2.3 of this Chapter 10, a responsible Customer may comply with the Standards set forth in this section 10.2.4 provided all of the following criteria are satisfied:

Criterion A

Mastercard determines that fewer than 30,000 Accounts are 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 computer-based 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 Member Information—Mastercard 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 10.2.2.1 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 10.2.6. 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 a written certification by an officer of the responsible Customer certifying 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 Merchants (or Agents); 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 breach was contained (including the steps taken to ensure that Account data are no longer at risk of compromise) must be provided to Mastercard with the officer certification; and
- The Merchant has newly validated or revalidated compliance with the PCI DSS. Documentation confirming such validation or revalidation must be provided to Mastercard with the officer certification.

Failure to comply with any obligation of the responsible Customer may result in the imposition of a noncompliance assessment as described in section 10.2.6.

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 certified by an officer of the responsible Customer as fully contained 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 Member Information—Mastercard 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 10.2.6.

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 10.2.6.

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 10.2.2.1 of this Chapter 10; and
- May impose an assessment of USD 25,000 upon the responsible Customer for failure to safeguard Account data.

Except as specifically set forth in this section 10.2.4, 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 10.2.4. 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 10.2.4.

10.2.5 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.

10.2.5.1 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.

10.2.5.2 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, ADC fraud recovery, 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 10.3.3 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*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*, found at 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 forensic 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 Member Information 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 Member Information application.

10.2.5.3 ADC Operational Reimbursement and ADC Fraud Recovery—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. ADC fraud recovery (FR) enables an Issuer to recover partial incremental magnetic-stripe (POS 90) and/or Hybrid POS Terminal

unable to process (POS 80) counterfeit fraud losses associated with an ADC Event. Mastercard determines ADC operational reimbursement and ADC fraud recovery.

Mastercard may invoke OR, or OR and FR (OR and FR together, the "reimbursement component"), for an ADC Event impacting 30,000 Mastercard Accounts or more. Participation in the reimbursement component of the ADC Program is optional for Issuers on a calendar year basis. Annually, each Issuer may choose to participate in the reimbursement component for the next following calendar year. An Issuer must choose to participate in the reimbursement component to be eligible to receive OR and/or FR with respect to an ADC Event that Mastercard deems to have occurred during that calendar year. For purposes of this section 10.2.5.3, 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.

Each Issuer that chooses to participate in the reimbursement component, as a condition of such participation, must agree to hold harmless and release Mastercard and, as applicable, each responsible Customer and each Agent of each responsible Customer from financial and other liability directly or indirectly related to an ADC Event that Mastercard deems to have occurred during that calendar year. Mastercard will collect an annual fee on or about the beginning of each calendar year from each Issuer that elects to participate in the reimbursement component of the ADC Program, as applicable to the Region. An Issuer that elects not to participate in the reimbursement component during a calendar year will be assessed a reduced annual fee for receiving ADC Alerts, as applicable to the Region.

Should Mastercard determine that an insufficient number of Issuers have opted to participate in the reimbursement component of the ADC Program in a calendar year, Mastercard will notify Customers of that determination; in such event, Issuers in each Region will be assessed a reduced annual fee for receiving ADC Alerts only, as applicable.

Following the conclusion of an investigation, the OR and/or FR liability, 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. If after the conclusion of any appeal, Mastercard determines that the responsible Customer has any financial liability related to the ADC Event, the responsible Customer may either agree to or refuse to agree to the determined amount. As a condition of agreeing to the determined amount, and with respect to the ADC Event, the responsible Customer must both:

- Execute and deliver to Mastercard within 14 calendar days of receipt of the final financial liability letter or a decision by Mastercard on the appeal, whichever is later, a release in a form and substance acceptable to Mastercard memorializing that the Customer agrees to not assert a claim arising from or related to the ADC Event against either Mastercard or any Issuer that receives OR and/or FR; and
- Deliver to Mastercard a release in a form and substance acceptable to Mastercard and executed by the Merchant (or other Agent) that the Merchant (or other Agent) agrees to not assert a claim arising from or related to the ADC Event against either Mastercard or any Issuer that receives OR and/or FR.

Mastercard subsequently will debit funds from the responsible Customer's account and disburse OR and/or FR to Issuers, as appropriate.

If the responsible Customer refuses to agree to the determined amount, each Issuer that has chosen to participate in the reimbursement component of the ADC Program for the year in which Mastercard determined the ADC Event to have occurred shall be released from its waiver of the right to assert claims related to or in connection with the ADC Event against the responsible Customer and/or the responsible Customer's Agent(s).

For additional information, see Chapter 6 of the *ADC User's Guide*.

In the event that the compromised entity is an electronic commerce (e-commerce) Merchant and only the Cardholder name, PAN, expiration date, and/or the CVC 2 data were compromised, only partial ADC operational reimbursement will be invoked.

Partial operational reimbursement and partial fraud recovery are available to an Issuer that is licensed to access the Manage My Fraud & Risk Programs application at the time of the ADC Event and has chosen to participate in the reimbursement component of the ADC Program for the calendar year in which Mastercard has deemed the ADC Event to have occurred. Mastercard reserves the right to determine whether any ADC Event is eligible for ADC operational reimbursement and/or ADC fraud recovery and to limit or "claw back" ADC operational reimbursement and/or ADC fraud recovery 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 and/or ADC fraud recovery 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 and ADC FR programs, 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 10.3.4), annual sales volume, and the factors set forth in section 10.2.5.2.

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.

10.2.5.4 Determination of Operational Reimbursement (OR)

NOTE: This section applies to Mastercard Transactions only.

Subject to section 10.2.5.3, 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 Card 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 Card 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. **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.

10.2.5.5 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 10.2.5.3, Mastercard determines an amount of incremental counterfeit fraud attributable to an ADC Event based on the fraud data reported to the System to Avoid Fraud Effectively (SAFE). 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 SAFE 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 SAFE 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 SAFE. Mastercard will determine the number of days that the Issuer has to report fraudulent Transactions to SAFE 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 SAFE.

  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 SAFE 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 SAFE.

  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 SAFE 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 SAFE 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 SAFE. Mastercard will determine the number of days that the Issuer has to report fraudulent Transactions to SAFE 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 SAFE.

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 SAFE 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 SAFE.

  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 SAFE 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 Card 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 Card 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.

10.2.6 Assessments and/or Disqualification for Noncompliance

If the Customer fails to comply with the procedures set forth in this section 10.2, 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 under this section 10.2.

10.2.7 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 10.2.2 and 10.2.3, 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 sections 10.2.2 or 10.2.3, but failed to do so, such documents or other information will not be considered by Mastercard in deciding the appeal.

10.3 Mastercard Site Data Protection (SDP) Program

NOTE: This section applies to Mastercard and Maestro Transactions.

The Mastercard Site Data Protection (SDP) Program is designed to encourage 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], and 3-D Secure Service Providers [3-DSSPs]) to protect against Account Data Compromise (ADC) Events. The SDP Program facilitates the identification and correction of vulnerabilities in security processes,

procedures, and website configurations. For the purposes of the SDP Program, TPPs, DSEs, PFs, SDWOs, DASPs, TSPs, TSs, and 3-DSSPs are collectively referred to as "Service Providers" in this chapter.

NOTE: Refer to section 10.2 of this manual for the definition of an Account Data Compromise Event.

An Acquirer must implement the Mastercard SDP Program by ensuring that its Merchants and Service Providers are compliant with the *Payment Card Industry Data Security Standard (PCI DSS)* and that all applicable third party-provided payment applications used by its Merchants and Service Providers are compliant with the *Payment Card Industry Payment Application Data Security Standard* (PCI PA-DSS), in accordance with the implementation schedule defined in section 10.3.1 of this manual. Going forward, the *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* will be components of the SDP Program; these documents set forth security Standards that Mastercard hopes will be adopted as industry standards across the payment brands.

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, a Merchant, or a Service Provider is the source of an ADC Event.

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

10.3.1 Payment Card Industry Security Standards

The *Payment Card Industry Data Security Standard*, the *Payment Card Industry Payment Application Data Security Standard*, the *Payment Card Industry Token Service Providers—Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens),* also known as the *PCI TSP Security Requirements*, and the *Payment Card Industry 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)*, also known as the *PCI 3DS Core Security Standard*, establish data security requirements. Compliance with the *Payment Card Industry Data Security Standard* is required for all Issuers, Acquirers, Digital Activity Customers, Merchants, Service Providers, and any other person or entity that a Customer permits, directly or indirectly, to store, transmit, or process Account data. Compliance with the *PCI TSP Security Requirements* is required for any Issuer that performs TSP services on its own behalf and any entity that performs or proposes to perform TSP Program Service as the TSP of a Customer. 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*.

Mastercard requires validation of compliance only for those entities specified in the SDP Program implementation schedule in section 10.3.4. All Merchants and Service Providers that use third party-provided payment applications must only use payment applications that are compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. Mastercard recommends that Merchants use a Qualified Integrator & Reseller (QIR) listed on the PCI Security Standards Council (SSC) website to implement a PCI PA-DSS-compliant payment application, 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 QIR engagement for third party-provided payment application implementation is defined in the *PCI QIR Program Guide*.

All Service Providers that use 3-D Secure (3DS) Software Development Kits (SDKs) must only use 3DS SDKs that are compliant with the *Payment Card Industry 3-D Secure—Security Requirements and Assessment Procedures for EMV 3-D Secure SDK*, also known as the *PCI 3DS SDK Security Standard*, as applicable. Mastercard recommends that any Merchant that performs or provides 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 SDKs listed on the PCI SSC website at www.pcisecuritystandards.org, as applicable.

The *Payment Card Industry Data Security Standard*, the *Payment Card Industry Payment Application Data Security Standard*, the *PCI PA-DSS Program Guide*, the *PCI QIR Program Guide*, the *PCI TSP Security Requirements*, the *PCI 3DS Core Security Standard*, the *PCI 3DS SDK Security Standard*, and other PCI Security Standards manuals are available on the PCI SSC website.

10.3.2 Compliance Validation Tools

Unless otherwise specified in the implementation schedule in section 10.3.4, Merchants and Service Providers must validate their compliance with the *Payment Card Industry Data Security Standard* and if applicable, the *PCI TSP Security Requirements* or the *PCI 3DS Core Security Standard*, by using the following tools:

Onsite Reviews

The onsite review evaluates Merchant or Service Provider compliance with the *Payment Card Industry Data Security Standard* and if applicable, the *PCI TSP Security Requirements*, or the *PCI 3DS Core Security Standard*. Onsite reviews are an annual requirement for Level 1 Merchants and for Level 1 Service Providers. Merchants may use an internal auditor or independent assessor recognized by Mastercard as acceptable. Service Providers must use an acceptable third-party assessor as defined on the SDP Program website. Onsite reviews must be conducted in accordance with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures* and if applicable, the *PCI TSP Security Requirements* or the *PCI 3DS Core Security Standard*.

The *Payment Card Industry Self-assessment Questionnaire*

The *Payment Card Industry Self-assessment Questionnaire* is available at no charge on the PCI SSC website. To be compliant, each Level 2, 3, and 4 Merchant, and each Level 2 Service Provider must generate acceptable ratings on an annual basis.

Network Security Scan

The network security scan evaluates the security measures in place at a website. To fulfill the network scanning requirement, all Level 1 to 3 Merchants and all Service Providers as required by the implementation schedule must conduct scans on a quarterly basis using a vendor listed on the PCI SSC website. To be compliant, scanning must be conducted in accordance with the guidelines contained in the *Payment Card Industry Data Security Standard Approved Scanning Vendors Program Guide*.

10.3.3 Acquirer Compliance Requirements

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

- For each Level 1, Level 2, and Level 3 Merchant, submit a semi-annual status report by email message to sdp@mastercard.com using the form provided on the SDP Program website. This submission form must be completed in its entirety and may include information on:
  - The name and primary contact information of the Acquirer
  - The name of the Merchant
  - The Merchant identification number of the Merchant
  - The number of Transactions that the Acquirer processed for the Merchant during the previous 12-month period
  - The Merchant's level under the implementation schedule provided in section 10.3.4 of this manual
  - The Merchant's compliance status with its applicable compliance validation requirements
  - The Merchant's anticipated compliance validation date **or** the date on which the Merchant last validated its compliance (the "Merchant Validation Anniversary Date")
- Communicate the SDP Program requirements to each Level 1, Level 2, and Level 3 Merchant, and validate the Merchant's compliance with the *Payment Card Industry Data Security Standard* by reviewing its *Payment Card Industry Self-assessment Questionnaire* and the Reports on Compliance (ROC) that resulted from network security scans and onsite reviews of the Merchant, if applicable.
- Communicate the SDP Program requirements to each Level 1 and Level 2 Service Provider, and ensure that Merchants use only compliant Service Providers.
- Effective 31 March 2019, 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.

In submitting a semi-annual SDP status report indicating that the Merchant has validated compliance within 12 months of the report submission date, the Acquirer certifies that:

1. The Merchant has, when appropriate, engaged and used the services of a data security firm(s) considered acceptable by Mastercard for onsite reviews, security scanning, or both.
2. Upon reviewing the Merchant's onsite review results, *Payment Card Industry Self-assessment Questionnaire*, or network scan reports, the Acquirer has determined that the Merchant is in compliance with the *Payment Card Industry Data Security Standard* requirements.
3. On an ongoing basis, the Acquirer will monitor the Merchant's compliance. If at any time the Acquirer finds the Merchant to be noncompliant, the Acquirer must notify the Mastercard SDP Department in writing at sdp@mastercard.com.

At its discretion and from time to time, Mastercard may also request the following information:

- Merchant principal data

- The name of any Level 1 or Level 2 Service Provider that performs Transaction processing services for the Merchant's Transactions
- Whether the Merchant stores Account data

When considering whether a Merchant stores Account data, Acquirers carefully should survey each Merchant's data processing environment. Merchants that do not store Account information in a database file still may accept payment Card information through a web page and therefore store Account data temporarily in memory files. According to the Mastercard data storage definition, any temporary or permanent retention of Account data is considered to be storage. A Merchant that does not store Account data never processes the data in any form, such as in the case of a Merchant that outsources its environment to a web hosting company, or a Merchant that redirects customers to a payment page hosted by a third-party Service Provider.

10.3.4 Implementation Schedule

All onsite reviews, network security scans, and self-assessments must be conducted according to the guidelines in section 10.3.2. For purposes of the SDP Program, Service Providers in this section refer to TPPs, DSEs, PFs, SDWOs, DASPs, TSPs, TSs, and 3-DSSPs.

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, 2, and 3 Merchants and all Service Providers that use any third party-provided payment applications must validate that each payment application used is listed on the PCI SSC website at www.pcisecuritystandards.org as compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. Mastercard recommends that Merchants use a QIR listed on the PCI SSC website to implement a PCI PA-DSS-compliant payment application, 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 QIR engagement for third party-provided payment application implementation is defined in the *PCI QIR Program Guide*.

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. Mastercard recommends that any Merchant that performs or provides 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 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 *Payment Card Industry Data Security Standard*:

- Any Merchant that has suffered a hack or an attack that resulted in an Account data compromise,
- 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.

To validate compliance, each Level 1 Merchant must successfully complete:

- An annual onsite assessment conducted by a PCI SSC-approved Qualified Security Assessor (QSA) or internal auditor, and
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV).

Level 1 Merchants that use internal auditors for compliance validation must ensure that primary internal auditor staff engaged in validating compliance with the *Payment Card Industry Data Security Standard* attend the PCI SSC-offered Internal Security Assessor (ISA) Program and pass the associated PCI SSC accreditation examination annually in order to continue to use internal auditors.

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 *Payment Card Industry Data Security Standard*:

- 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 self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

Each Level 2 Merchant must ensure that staff engaged in self-assessing the Merchant's compliance with the *Payment Card Industry Data Security Standard* attend the PCI SSC-offered ISA Program and pass the associated PCI SSC accreditation examination annually in order to continue the option of self-assessment for compliance validation. Level 2 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

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 *Payment Card Industry Data Security Standard*:

- 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 self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

Level 3 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

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 *Payment Card Industry Data Security Standard* is required for a Level 4 Merchant, although validation of compliance (and all other Mastercard SDP Program Acquirer requirements set forth in section 10.3.3, except the validation of an established Level 4 Merchant risk management program [effective 31 March 2019]) 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 *Payment Card Industry Data Security Standard* by successfully completing:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

Level 4 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

If a Level 4 Merchant has validated its compliance with the *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* as described in this section, the Acquirer may, at its discretion, fulfill the reporting requirements described in section 10.3.3.

Level 1 Service Providers

A Level 1 Service Provider is any TPP, SDWO, DASP, TSP, or 3-DSSP (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 *Payment Card Industry Data Security Standard*, each TSP must additionally validate compliance with the *PCI TSP Security Requirements*, and each 3-DSSP must validate compliance with the *PCI 3DS Core Security Standard* by successfully completing:

- An annual onsite assessment by an appropriate PCI SSC-approved QSA, and
- Quarterly network scans conducted by a PCI SSC ASV.

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

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 *Payment Card Industry Data Security Standard* by successfully completing:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

As an alternative to validating compliance with the *Payment Card Industry Data Security Standard*, 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.

Mastercard recommends that each Level 2 Service Provider demonstrate to Mastercard its compliance with the DESV appendix of the PCI DSS.

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 10.1.

Table 10.1—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

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 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, or 3-DSSP as a Service Provider; or termination of the Acquirer as a Customer as provided in Rule 2.1.2 of the *Mastercard Rules* manual.

The Acquirer must provide compliance action plans and semi-annual compliance status reports for each Level 1, Level 2, and Level 3 Merchant using the SDP Acquirer Submission and Compliance Status Form, available on the Acquirer page of the SDP Program website or by contacting the Mastercard SDP Department at sdp@mastercard.com.

Acquirers must complete the form(s) in their entirety and submit the form(s) by email message to sdp@mastercard.com, as indicated below.

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

Late submission or failure to submit the required form(s) may result in an additional assessment to the Acquirer as described for Category A violations in Rule 2.1.4 of the *Mastercard Rules* manual.

10.3.4.1 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, pursuant to which the Merchant:

- Validates 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 an onsite assessment conducted by a PCI SSC-approved QSA, or by conducting an onsite assessment using internal resources that have been trained and certified through the PCI SSC-offered ISA Program.

  - A Level 2 Merchant must validate compliance using a Self-Assessment Questionnaire (SAQ) completed by internal resources that have been trained and certified through the PCI SSC-offered ISA Program. Alternatively, the Level 2 Merchant may validate PCI DSS compliance by way of an onsite assessment.
- Annually revalidates compliance with milestones one and two using an SAQ. The SAQ must be completed by internal staff trained and currently certified through the PCI SSC-offered ISA Program.

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 Card 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 within the last 12 months. 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:
www.pcisecuritystandards.org/education/prioritized.shtml

10.3.4.2 Mastercard PCI DSS Compliance Validation Exemption Program

A qualifying Level 1, Level 2, or Level 4 Merchant may participate in the Mastercard PCI DSS Compliance Validation Exemption Program (the "Exemption Program"), which exempts the Merchant from the requirement to annually validate 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 validated its compliance with the PCI DSS within the previous twelve (12) months or, alternatively, has submitted to its Acquirer, and the Acquirer has submitted to Mastercard, a defined remediation plan satisfactory to Mastercard designed to ensure that the Merchant achieves PCI DSS compliance based on a PCI DSS gap analysis;
2. The Merchant does not store Sensitive Card Authentication Data. The Acquirer must notify Mastercard through compliance validation reporting of the status of Merchant storage of Sensitive Card Authentication Data;

3. The Merchant has not been identified by Mastercard as having experienced an ADC Event during the prior twelve (12) months;
4. The Merchant has established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements; and
5. The Merchant has satisfied either 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 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; **OR**
    b. The Merchant has implemented a point-to-point encryption (P2PE) solution listed on the PCI SSC website.

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 and Mail Order/Telephone Order (MO/TO) acceptance channels, must continue to validate its PCI DSS compliance in accordance with the Mastercard SDP implementation schedule.

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

10.3.4.3 Mandatory Compliance Requirements for Compromised Entities

Under the audit requirement set forth in section 10.2.2.1, the Acquirer must ensure that a detailed forensics evaluation is conducted.

At the conclusion of the forensics evaluation, 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 QSA and the ASV that conducted the forensics evaluation;
- The entity's current level of compliance; and
- A gap analysis providing detailed steps required for the entity to achieve full compliance.

As soon as practical, but no later than 60 calendar days from the conclusion of the forensics evaluation, the compromised entity or its Acquirer must provide evidence from a QSA and an ASV that the compromised entity has achieved full compliance with the *Payment Card Industry Data Security Standard* and if applicable, the *PCI TSP Security Requirements* or the *PCI 3DS Core Security Standard*.

Such evidence (for example, a completed PCI SSC Attestation of Compliance [AOC] and a network scan AOC conducted by a PCI SSC ASV) must be submitted to Mastercard by email message to pci_adc@mastercard.com.

Failure to comply with these requirements may result in SDP noncompliance assessments as described in section 10.3.4. Any Merchant or Service Provider that has suffered a confirmed ADC Event will be automatically reclassified to become a Level 1 Merchant or a Level 1 Service Provider, respectively. All compliance validation requirements for such Level 1 entities will apply.

10.4 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.

10.4.1 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.

10.4.2 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.

10.4.3 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 10.4. 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.

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 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 and associate business owners for each Merchant.
- Acquirers may designate regions and countries for database searches.
- 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.
- MATCH processes data submitted by Acquirers once a day and provides daily detail response files.
- Acquirers may add the name of the Service Provider associated with signing the Merchant.
- Acquirers may 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 direct communication with the listing Acquirer, 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					=	√

Field	+	Field	+	Field	=	Match
Phone Number (Merchant)					=	√
Alternate Phone Number (Merchant)					=	√
Merchant National Tax ID	+	Country			=	√
Merchant State Tax ID	+	State			=	√
Merchant Street Address	+	City	+	State[4]	=	√
Merchant Street Address	+	City	+	Country[5]	=	√
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					=	√
PO National ID					=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO State[4]	=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO Country[5]	=	√
PO Driver's License (DL) Number	+	DL State[4]			=	√
PO Driver's License Number	+	DL Country[5]			=	√

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.

[2] If country is USA.
[3] If country is not USA.

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					=	√
Merchant Street Address	+	City	+	State	=	√
Merchant Street Address	+	City	+	Country	=	√
Principal Owner's (PO) First Name	+	Last Name			=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO State[6]	=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO Country[7]	=	√

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. 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

[4] If country is USA.
[5] If country is not USA.
[6] 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.

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.

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 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

An Acquirer should retain all MATCH records returned by Mastercard to substantiate that the Acquirer complied with the required procedures. Mastercard recommends that the Acquirer retain these records in a manner that allows for easy retrieval.

Merchant records remain on the MATCH system for five years. Each month, MATCH automatically purges any Merchant information that has been in the database for five years.

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 matchhelp@mastercard.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.

MATCH Reason Code	Description
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***
07	***Fraud Conviction*** There was a criminal fraud conviction of a principal owner or partner of the Merchant.
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.

MATCH Reason Code	Description
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.

11.7.1 Privacy and Data Protection

An Acquirer or Merchant that stores, transmits, or processes Personal Data[7], including Criminal Data[7] and Sensitive Data[7], of a resident of the European Economic Area or that is otherwise subject to EU Data Protection Law[7] must comply with the Standards set forth in Appendix D of this manual pertaining to MATCH Activity conducted in the Europe Region.

[7] 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

Chapter 13 Global Risk Management Program

This chapter describes the Global Risk Management Program Standards and applies to all Mastercard Customers, Service Providers, and Payment Facilitators.

13.1 About the Global Risk Management Program

The Global Risk Management Program is a holistic approach by which Mastercard identifies, analyzes, evaluates, responds to, and monitors risks to which Customers and Service Providers may be exposed on an ongoing basis.

The Global Risk Management Program also determines the effectiveness of existing fraud loss controls and other risk reduction measures and assists Mastercard Customers and Service Providers in identifying specific areas where such measures may be inadequate.

In addition, the Global Risk 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 Global Risk 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 Risk Reviews** for Mastercard Principal Customers. A Maestro Customer identified by Mastercard as a Group 3 Issuer pursuant to the Maestro Issuer Loss Control Program may also be required to undergo a Customer Risk Review.

A Customer may also choose to participate in **Customer Consultative Reviews**.

NOTE: Mastercard may conduct a review through one or more channels, including but not limited to, a telephone interview, a questionnaire, or an on-site evaluation.

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 on-site reviews to evaluate the controls that the Service Provider has in place to mitigate risks.

Mastercard reserves the right for Global Risk Management Program staff to conduct an on-site review of any Service Provider at any time.

Mastercard will 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

Appendix B Omitted

Appendix C Omitted

Appendix D MATCH Privacy and Data Protection Standards

This appendix describes the privacy and data protection Standards for the Mastercard Alert to Control High-risk (Merchants) (MATCH™) system 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 Mastercard and its Customers (collectively referred to in this appendix as the "Parties") in the context of the Mastercard Alert to Control High-risk (Merchants) (MATCH™) system.

D.2 Scope

The Standards in this appendix supplement the privacy and data protection Standards contained in this manual and requirements to the extent that the requirements pertain to the Processing of Personal Data subject to EU Data Protection Law in the context of MATCH. 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.

Data Subject

A Cardholder, a Merchant, or other natural person whose Personal Data are Processed by or on behalf of Mastercard, a Customer, or a Merchant. In the context of MATCH, a Data Subject may be a Merchant principal owner.

EU Data Protection Law

The EU General Data Protection Regulation 2016/679 (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 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).

General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).

Mastercard Binding Corporate Rules (Mastercard BCRs)

The Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available at https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf.

Personal Data

Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. In the context of MATCH, these data may include Merchant principal owner details such as the name, address, phone number, driver's license number, and national ID number, in accordance with applicable law.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Processor

The entity which Processes Personal Data on behalf of a Controller.

Processing of Personal Data (or Processing/Process)

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.

Sensitive Data

Any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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.

D.4 Acknowledgment of Roles

Mastercard 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. Mastercard 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 Mastercard, for the purpose of developing enhanced or incremental risk information to aid in its own determination of risk in its Merchant acquiring business.
- Mastercard is a Controller for any Processing for the purpose of operating MATCH, including product development, support and maintenance, and making MATCH available to its Customers and other third parties in accordance with Chapter 11 of this manual, and for any purpose listed in Rule 3.10, "Confidential Information of Customers", of the *Mastercard Rules* manual, including internal research, fraud, security, and risk management.

D.5 Mastercard and Customer Obligations

Mastercard and each Customer 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 Merchants and related Data Subjects whose information a Customer adds to MATCH, including the Processing for which Mastercard 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 Processing of Personal Data, in a timely manner and at the minimum with the elements required under EU Data Protection Law, (ii), as appropriate, the existence of Mastercard BCRs.
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 of (i) access, (ii) rectification, (iii) erasure, (iv) data portability, (v) restriction of Processing, (vi) objection to the Processing, and (vii) the rights related to automated decision-making and profiling, if and as required under EU Data Protection Law. The Customer agrees and warrants that it will respond to such requests only in consultation with Mastercard. Mastercard agrees to cooperate with the Customer in responding to such requests.

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. Comply with any applicable requirements under EU Data Protection Law if it engages in automated decision-making or profiling in the context of MATCH.
7. Will not add any Sensitive Data, Criminal Data, and/or government identification information to MATCH, unless as permitted under applicable law.

D.6 Data Transfers

A Customer may transfer the Personal Data Processed in connection with MATCH outside of the EEA in accordance with EU Data Protection Law.

Mastercard may transfer the Personal Data Processed in connection with MATCH outside of the EEA 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. Mastercard will abide by the Mastercard BCRs when Processing Personal Data in the context of MATCH.

D.7 Data Disclosures

Mastercard and its Customers must ensure that they will only disclose Personal Data Processed in the context of MATCH 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. Mastercard must ensure that it will only disclose Personal Data in accordance with the Mastercard BCRs.

D.8 Security Measures

Mastercard 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, Mastercard 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

Mastercard 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

Each Party must notify the other Party when a Personal Data Breach occurs that relates to Personal Data Processed in the context of MATCH and for which the other Party is a Controller, without undue delay, and no later than 48 hours after having become aware of a Personal Data Breach.

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

Mastercard and its Customers will use their best efforts to reach an agreement on whether and how to notify each other when a Personal Data Breach occurs, and 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

Mastercard 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 Mastercard must comply with the Mastercard BCRs.

Upon prior written request, Mastercard 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 this manual, Mastercard 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 Mastercard and each responsible Customer may be held liable for the entire damage in order to ensure effective compensation of the Data Subject.

If Mastercard paid full compensation for the damage suffered, Mastercard 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 Applicable Law and Jurisdiction

Mastercard and its Customers agree that the Standards in this appendix and the Processing of Personal Data will be governed by the law of Belgium and that any dispute will be submitted to the Courts of Brussels.

D.15 Termination of MATCH Use

Mastercard and its Customers agree that the Standards in this appendix are no longer applicable to a Customer upon the termination of such Customer's use of MATCH.

D.16 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.

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.

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 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; and
- 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 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 lawfully undertaken only pursuant to a License granted by the Corporation. *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.

Area of Use

The country or countries in which a Customer is Licensed to use the Marks and conduct Activity, and, as a rule, set forth in the License or in an exhibit to the License.

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 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 a Transaction with a Card 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).

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.

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, as set forth in Rule 6.1.3.2 of the *Mastercard Rules* manual, and identified with a BIN/IIN associated with a Portfolio designated by the Corporation as a Cirrus Portfolio in its routing tables.

Cirrus Brand Mark

A Mark consisting of the Cirrus Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Corporation is the exclusive owner of the Cirrus Brand Mark.

Cirrus Card

A Card that provides access to a Cirrus Account.

Cirrus Customer

A Customer that has been granted a Cirrus License in accordance with the Standards.

Cirrus Payment Application

A Payment Application that stores Cirrus Account data.

Cirrus Word Mark

A Mark consisting of the word "Cirrus" followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent. "Cirrus" must appear in English and be spelled correctly, with the letter "C" capitalized. "Cirrus" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. The Corporation is the exclusive owner of the Cirrus Word Mark.

Competing ATM Network

A Competing International ATM Network or a Competing North American ATM Network, as the case may be.

Competing 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.

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, or Sponsored Digital Activity Entity. *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, use of any Mark, or any such matters. By way of example and not limitation, the Quarterly Mastercard Report (QMR) is a Customer Report.

Data Storage Entity (DSE)

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as DSE Program Service.

Device Binding

The process by which a Wallet Token Requestor binds a Mastercard Token corresponding to a Cardholder's Account to that Cardholder's Mobile Payment Device, which may consist of:

- The provisioning of the Token and its associated encryption keys into the secure element within the Mobile Payment Device;
- The loading of an application for a remotely-managed secure server into the Mobile Payment Device and the successful communication of the device with the application; or
- Other methodology acceptable to the Corporation.

Digital Activity(ies)

The undertaking of any lawful act pursuant to approval by the Corporation as set forth in a Digital Activity Agreement or other written documentation. Participation in the Mastercard Digital Enablement Service as a Wallet Token Requestor is a Digital Activity.

Digital Activity Agreement

The contract between the Corporation and a Digital Activity Customer granting the Digital Activity Customer the right to participate in Digital Activity and a limited License to use one or more of the Marks in connection with such Digital Activity, in accordance with the Standards.

Digital Activity Customer

A Customer that participates in Digital Activity pursuant to a Digital Activity Agreement and which may not issue Cards, acquire Transactions, or Sponsor any other Customer into the Corporation.

Digital Activity Service Provider (DASP)

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* as DASP Program Service.

Digital Activity Sponsoring Customer

A Principal Customer or Digital Activity Customer that sponsors a Sponsored Digital Activity Entity to participate in Digital Activity.

Digital Goods

Any goods that are stored, delivered, and used in electronic format, such as, by way of example but not limitation, books, newspapers, magazines, music, games, game pieces, and software (excluding gift cards). The delivery of a purchase of Digital Goods may occur on a one-time or subscription basis.

Digital Wallet

A Pass-through Digital Wallet or a Staged Digital Wallet.

Digital Wallet Operator (DWO)

A Service Provider that operates a Staged Digital Wallet or a Customer that operates a Pass-through Digital Wallet. A Merchant that stores Mastercard or Maestro Account data solely on its own behalf to effect Transactions initiated by the consumer is not deemed to be a DWO.

Digital Wallet Operator Mark, DWO Mark

A Mark identifying a particular Pass-through Digital Wallet and/or Staged Digital Wallet, and which may be displayed at the POI to denote that a retailer, or any other person, firm, or corporation, accepts payments effected by means of that Pass-through Digital Wallet and/or Staged Digital Wallet. A "Staged DWO Mark" and a "Pass-through DWO Mark" are both types of DWO Marks.

Digital Wallet Operator (DWO) Security Incident, DWO Security Incident

Any incident pertaining to the unintended or unlawful disclosure of Personal Data in connection with such Personal Data being processed through a DWO.

Digitization, Digitize

Data preparation performed by, or on behalf of, an Issuer prior to the provisioning of Account credentials, 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.

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.

Identification & Verification (ID&V)

The identification and verification of a person as the Cardholder to whom the Issuer allocated the Account PAN to be Tokenized.

Independent Sales Organization (ISO)

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as ISO Program Service.

Interchange System

The computer hardware and software operated by and on behalf of the Corporation for the routing, processing, and settlement of 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.

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. 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, as set forth in Rule 6.1.2.1 of the *Mastercard Rules* manual, and identified with a BIN/IIN associated with a Portfolio designated by the Corporation as a Maestro Portfolio in its routing tables.

Maestro Brand Mark

A Mark consisting of the Maestro Word Mark as a custom lettering legend placed within the Corporation's interlocking circles device. The Corporation is the exclusive owner of the Maestro Brand Mark.

Maestro Card

A Card that provides access to a Maestro Account.

Maestro Customer

A Customer that has been granted a Maestro License in accordance with the Standards.

Maestro Payment Application

A Payment Application that stores Maestro Account data.

Maestro Word Mark

A Mark consisting of the word "Maestro" followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent. "Maestro" must appear in English and be spelled correctly, with the letter "M" capitalized. "Maestro" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. Maestro is the exclusive owner of the Maestro Word Mark.

Magnetic Stripe Mode Contactless Transaction

A Contactless Transaction in which the Terminal receives static and dynamic data from the chip and constructs messages that can be transported in a standard magnetic stripe message format, in compliance with the Standards.

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 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-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.

Mastercard Biometric Card

A Mastercard or Maestro Chip Card containing a fingerprint sensor and compliant with the Corporation's biometric Standards.

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 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 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 Token

A Token allocated from a Mastercard Token Account Range that the Corporation has designated to an Issuer and that corresponds to an Account PAN. 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 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.

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 letters "M" and "C" capitalized. "Mastercard" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language. The Corporation is the exclusive owner of the Mastercard Word Mark.

Member, Membership

A financial institution or other entity that is approved to be a Mastercard Customer in accordance with the Standards and which, as a Mastercard Customer, has been granted membership ("Membership") in and has become a member ("Member") of the Corporation. "Membership" also means "Participation".

Merchandise Transaction

The purchase by a Cardholder of merchandise or a service, but not currency, in an approved category at an ATM Terminal and dispensed or otherwise provided by such ATM Terminal. A Merchandise Transaction is identified with MCC 6012 (Merchandise and Services—Customer Financial Institution), unless otherwise specified.

Merchant

A retailer, or any other person, firm or corporation that, pursuant to a Merchant Agreement, agrees to accept Cards when properly presented.

Merchant Agreement

An agreement between a Merchant and a Customer that sets forth the terms pursuant to which the Merchant is authorized to accept Cards.

Merchant 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.

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).

Multi-Account Chip Card

A Chip Card with more than one Account encoded in the chip.

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.

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, or both granted to a Customer by the Corporation. For a Mastercard Customer, Participation is an alternative term for Membership.

Pass-through Digital Wallet

Functionality which can be used at more than one Merchant, and by which the Pass-through Digital Wallet Operator stores Mastercard or Maestro Account data provided by the Cardholder to the DWO for purposes of effecting a payment initiated by the Cardholder to a Merchant or Submerchant, and upon the performance of a Transaction, transfers the Account data to the Merchant or Submerchant or to its Acquirer or the Acquirer's Service Provider.

Pass-through Digital Wallet Operator (DWO)

A Digital Activity Customer or other Customer, approved by the Corporation to engage in Digital Activity, that operates a Pass-through Digital Wallet.

Payment Account Reference (PAR)

A unique non-financial alphanumeric value assigned to an Account PAN that is used to link the Account PAN to all of its corresponding Tokens.

Payment Application

A package of code and data stored in a Card, an Access Device, a server, or a combination of Access Device and server, that when exercised outputs a set of data that may be used to effect a Transaction, in accordance with the Standards. A Mastercard Payment Application, Maestro Payment Application, and Cirrus Payment Application is each a Payment Application.

Payment Facilitator

A Service Provider registered by an Acquirer to facilitate the acquiring of Transactions by the Acquirer from Submerchants, and which in doing so, performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as PF Program Service.

Personal Data

Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity.

Point of Interaction (POI)

The location at which a Transaction occurs, as determined by the Corporation.

Point-of-Sale (POS) Terminal

An attended or unattended device located in or at a Merchant's premises, including an MPOS Terminal, that enables a Cardholder to effect a Transaction for the purchase of products or services sold by such Merchant with a Card and/or Access Device, or attended device located in the premises of a Customer or its authorized agent that facilitates a Manual Cash Disbursement Transaction, including 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 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.

Program

A Customer's Card issuing program, Merchant acquiring program, ATM Terminal acquiring program, Digital Activity program, or all.

Program Service

Any service described in Rule 7.1 of the *Mastercard Rules* manual or elsewhere 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.

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.

Rules

The Standards set forth in this manual.

Service Provider

A person that performs Program Service. The Corporation has the sole right to determine whether a person is or may be a Service Provider and if so, the category of Service Provider. A Service Provider is an agent of the Customer that receives or otherwise benefits from Program Service, whether directly or indirectly, performed by such Service Provider.

Service Provider Registration Facilitator

A Service Provider that performs Service Provider identification and registration services.

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 intended to solicit the enrollment of a person as a Cardholder 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 such event, the Principal or Association is the Sponsor of the Affiliate and the Affiliate is Sponsored by the Principal or Association. "Sponsorship" means the Sponsoring of a Customer.

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.

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.

Sub-licensee

A person authorized in writing to use a Mark either by a Licensee in accordance with the Standards or by the Corporation.

Submerchant

A merchant that, pursuant to an agreement with a Payment Facilitator, is authorized to accept Cards when properly presented.

Submerchant Agreement

An agreement between a Submerchant and a Payment Facilitator that sets forth the terms pursuant to which the Submerchant is authorized to accept Cards.

Terminal

Any attended or unattended device that meets the Corporation requirements for the electronic capture and exchange of Card data and that permits a Cardholder to effect a Transaction in accordance with the Standards. An ATM Terminal, Bank Branch Terminal, and POS Terminal is each a type of Terminal.

Third Party Processor (TPP)

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *Mastercard Rules* manual as TPP Program Service.

Token

A numeric value that (i) is a surrogate for the primary account number (PAN) used by a payment card issuer to identify a payment card account; (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.

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 (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

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. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

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 Publications Support page available on Mastercard Connect™. Go to Publications Support for centralized information.