



Security Rules and Procedures

24 February 2012

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 Customer Operations Services 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.

Billing

For printed documents, MasterCard will bill principal Customers. Please refer to the appropriate MasterCard Consolidated Billing System (MCBS) document for billing-related information.

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 OnLine®. Go to Publications Support for centralized information.

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 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 Customers’ reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

Publication Code

SPME

Table of Contents

Definitions	1
Chapter 1 Customer Obligations.....	1-i
1.1 Compliance with the Standards	1-1
1.2 Conflict with Law	1-1
1.3 The Security Contact	1-1
Chapter 2 Omitted.....	2-i
Chapter 3 MasterCard Card and TID Design Standards.....	3-i
3.8 Mobile Payment Devices.....	3-1
3.9 Card Validation Code (CVC)	3-1
3.9.4 Acquirer Requirements for CVC 2	3-1
3.10 Service Codes	3-2
3.10.1 Issuer Information	3-2
3.10.2 Acquirer Information	3-2
3.10.3 Valid Service Codes	3-3
3.10.4 Additional Service Code Information	3-4
3.11 Transaction Information Documents (TIDs).....	3-5
3.11.1 Formset Contents	3-6
3.11.2 Point-of-Sale (POS) Terminal Receipt Contents	3-6
3.11.3 Standard Wording.....	3-7
3.11.4 Primary Account Number Truncation and Expiration Date Omission	3-8
Chapter 4 Terminal and PIN Security Standards.....	4-i
4.1 Personal Identification Numbers (PINs)	4-1
4.3 PIN Verification	4-1
4.5 PIN Encipherment.....	4-1
4.6 PIN Key Management	4-2
4.6.1 PIN Transmission between Customer Host Systems and the Interchange System.....	4-2
4.6.2 On-behalf Key Management	4-3
4.7 PIN at the Point of Interaction	4-4
4.8 Hybrid Terminal Security Standards.....	4-4
4.8.1 Hybrid Terminals Supporting Offline PIN	4-5

Table of Contents

4.9 PIN Entry Device Standards	4-5
4.10 Wireless POS Terminals and Internet/Stand-alone IP-enabled POS Terminal Security Standards	4-6
4.11 POS Terminals Using Electronic Signature Capture Technology (ESCT)	4-7
4.12 Component Authentication	4-7
4.13 Triple DES Migration Standards.....	4-8
Chapter 5 Card Recovery and Return Standards.....	5-i
5.1 Card Recovery and Return	5-1
5.1.1 Point-of-Interaction (POI) Card Retention	5-1
Chapter 6 Fraud Loss Control Standards	6-i
6.2 Fraud Loss Control Program Standards	6-1
6.2.2 Acquirer Fraud Loss Control Programs.....	6-1
6.3 Counterfeit Card Fraud Loss Control Standards	6-1
6.3.1 Counterfeit Card Notification.....	6-1
Chapter 7 Merchant Screening and Monitoring Standards	7-i
7.1 Screening New Merchants.....	7-1
7.1.1 Evidence of Compliance with Screening Procedures	7-1
7.1.2 Retention of Investigative Records	7-2
7.1.3 Assessments for Noncompliance with Screening Procedures.....	7-3
7.1.4 Screening Limitations	7-3
7.2 Ongoing Merchant Monitoring and Education.....	7-3
7.2.1 Merchant Monitoring.....	7-4
7.2.2 Additional Requirements for Certain Merchant Categories.....	7-4
7.2.3 Merchant Education	7-4
Chapter 8 Merchant Fraud Control Programs	8-i
8.1 Presenting Valid Transactions.....	8-1
8.1.1 Notifying MasterCard—Acquirer Responsibilities	8-1
8.1.2 Notifying MasterCard—Issuer Responsibilities	8-1
8.1.3 MasterCard Audit.....	8-1
8.2 Global Merchant Audit Program	8-3
8.2.1 Acquirer Responsibilities	8-4
8.2.2 Tier 3 Special Merchant Audit	8-5
8.2.3 Chargeback Responsibility	8-7
8.2.4 Exclusion from the Global Merchant Audit Program.....	8-8

8.2.5 Notification of Merchant Identification.....	8-10
8.2.6 Merchant Online Status Tracking (MOST) System.....	8-11
8.3 Excessive Chargeback Program.....	8-13
8.3.1 Definitions.....	8-13
8.3.2 Reporting Requirements.....	8-13
8.3.3 Assessments.....	8-15
8.3.4 Issuer Reimbursement.....	8-17
8.4 Cardholder-Merchant Collusion (CMC) Program.....	8-17
8.4.1 Issuer Notification to MasterCard.....	8-19
8.4.2 MasterCard Audit.....	8-20
8.4.3 Acquirer Investigation and Response.....	8-20
8.4.4 MasterCard Notification to Issuers.....	8-21
8.4.5 Issuer Obligation to Assist in MasterCard Audit.....	8-21
8.4.6 MasterCard Evaluation.....	8-22
8.4.7 Issuer Post-Audit Reporting Procedures.....	8-22
8.4.8 Issuer Recovery Claim Filing Process.....	8-23

Chapter 9 MasterCard Registration Program 9-i

9.1 MasterCard Registration Program Overview.....	9-1
9.2 General Registration Requirements.....	9-1
9.2.1 Merchant Registration Fees and Noncompliance Assessments.....	9-3
9.2.2 Service Provider Registration Noncompliance Assessments.....	9-3
9.3 General Monitoring Requirements.....	9-4
9.4 Additional Requirements for Specific Merchant Categories.....	9-4
9.4.1 Key-entry Telecom Merchants.....	9-4
9.4.2 Other Telecom Merchants and Transactions.....	9-5
9.4.3 Electronic Commerce Adult Content (Videotext) Merchants.....	9-6
9.4.4 Non-face-to-face Gambling Merchants.....	9-6
9.4.5 Prescription Drug and Tobacco Merchants.....	9-8
9.4.6 State Lottery Merchants (U.S. Region Only).....	9-9

Chapter 10 Account Data Protection Standards and Programs 10-i

10.1 Account Data Protection Standards.....	10-1
10.2 Account Data Compromise Events.....	10-1
10.2.1 Policy Concerning Account Data Compromise Events and Potential Account Data Compromise Events.....	10-2
10.2.2 Responsibilities in Connection with ADC Events and Potential ADC Events.....	10-3
10.2.3 Forensic Report.....	10-6

Table of Contents

10.2.4 MasterCard Determination of ADC Event or Potential ADC Event	10-8
10.2.5 Assessments for Noncompliance	10-11
10.3 MasterCard Site Data Protection (SDP) Program	10-12
10.3.1 Payment Card Industry Data Security Standards.....	10-12
10.3.2 Compliance Validation Tools.....	10-13
10.3.3 Acquirer Compliance Requirements	10-13
10.3.4 Implementation Schedule.....	10-15
10.4 Connecting to MasterCard—Physical and Logical Security Requirements	10-21
10.4.1 Minimum Security Requirements.....	10-21
10.4.2 Additional Recommended Security Requirements	10-22
10.4.3 Ownership of Service Delivery Point Equipment.....	10-22
Chapter 11 MATCH System.....	11-i
11.1 MATCH Overview	11-1
11.1.1 System Features.....	11-1
11.1.2 How does MATCH Search when Conducting an Inquiry?	11-2
11.2 MATCH Standards	11-4
11.2.1 Certification	11-5
11.2.2 When to Add a Merchant to MATCH.....	11-5
11.2.3 Inquiring about a Merchant.....	11-6
11.2.6 MATCH Record Retention.....	11-6
11.4 Merchant Removal from MATCH.....	11-6
11.5 MATCH Reason Codes	11-7
11.5.1 Reason Codes for Merchants Listed by the Acquirer	11-7
Chapter 12 Omitted.....	12-i
Chapter 13 Fraud Management Program (FMP)	13-i
13.1 About FMP	13-1
13.1.2 FMP Level 2 Service Provider Reviews.....	13-1
Chapter 14 Omitted.....	14-i
Chapter 15 Omitted.....	15-i
Appendix A Omitted	A-i
Appendix B Formset Specifications.....	B-i

B.1 MasterCard Formset Specifications	B-1
B.1.1 Formset Physical Dimensions	B-1
B.1.2 Number of Copies and Retention Requirements.....	B-1
B.1.3 Paper Stock Characteristics	B-1
B.1.4 Color of Interchange Copy	B-1
B.1.5 Carbon.....	B-1
B.1.6 Registration Mark	B-2
B.1.7 Formset Numbering.....	B-2
B.1.8 Information Slip Specifications	B-3
B.2 Formset Printing Standards	B-3
B.2.1 Retail Sale, Credit, and Cash Disbursement Formsets.....	B-3
B.2.2 Information Slip Formsets.....	B-4
B.2.3 Imprinters	B-4
Appendix C Omitted	C-i
Appendix D Omitted	D-i

Definitions

The following terms used in the *Security Rules and Procedures* manual have the meanings set forth below.

Access Device

A means other than a Card by which a Cardholder may access a MasterCard®, Debit MasterCard®, or MasterCard® Electronic™ account in accordance with the Standards. (See Card.)

Acquirer

A Customer in its capacity as an acquirer of a Transaction from a Merchant.

Activity(ies)

The undertaking of any act that can be lawfully undertaken only pursuant to License by the Corporation.

Affiliate Member, Affiliate

A financial institution that is eligible and approved to be a Member pursuant to MasterCard Rule 1.1.3, and is Sponsored by a Principal or Association. "Affiliate" is an alternative term for Affiliate Member. An Affiliate Member is also referred to as a Customer.

Association Member, Association

An entity that is eligible and approved to be a Member pursuant to MasterCard Rule 1.1.1. "Association" is an alternative term for Association Member. An Association Member is also referred to as a Customer.

Board, Board of Directors

The Board of Directors of MasterCard International Incorporated and MasterCard Incorporated.

Bylaws

The bylaws of MasterCard International Incorporated.

Card

A card issued by a Customer pursuant to License and in accordance with the Standards that provides access to a MasterCard, Debit MasterCard, or MasterCard Electronic account. Unless otherwise stated herein, Standards applicable to a Card are also applicable to an Access Device and a Mobile Payment Device.

Cardholder

The authorized user of a Card issued by a Customer.

Corporation

MasterCard International Incorporated and its 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 officer(s) or other employee(s) 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 or by the MasterCard Incorporated Certificate of Incorporation or by the MasterCard International 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.

Customer

An alternative term for Member. A Customer may be a Principal Member, an Association Member, or an Affiliate Member.

Data Storage Entity (DSE)

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

Independent Sales Organization (ISO)

A Service Provider that performs any one or more of the services described in MasterCard Rule 7.1 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 Worldwide Network, the Regional Service Center (RSC), the Regional Clearing Management System (RCMS), the Global Clearing Management System (GCMS), and the Settlement Account Management (S.A.M.) system.

Issuer

A Customer in its capacity as an issuer of a Card. For the purpose of this definition, an Issuer also means a principal debit Licensee and an affiliate debit Licensee.

License, Licensed

The contract between the Corporation and a Customer granting the Customer the right to use one or more of the Mark(s) in accordance with the Standards. To be “Licensed” means to have such a right pursuant to a License.

Marks

The names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks, including but not limited to the MasterCard Brand Mark and the MasterCard Word Mark, that MasterCard International Incorporated and/or its affiliates or subsidiaries own, manage, license, or otherwise control and make available for use by Customers and other authorized entities. A “Mark” means any one of the Marks.

MasterCard

MasterCard International Incorporated.

MasterCard Brand Mark

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 Rule

A Standard set forth in the *MasterCard Rules* manual.

MasterCard Word Mark

The word “MasterCard,” which should be followed by a registered trademark ® symbol or the local law equivalent. The Corporation is the exclusive owner of the MasterCard Word Mark.

Member, Membership

A financial institution or other entity that has been granted membership in and has become a member of the Corporation in accordance with the Standards. “Membership” means membership in the Corporation.

Merchant

A commercial entity or person that, pursuant to a Merchant Agreement, is authorized 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.

Mobile Payment Device

A Cardholder-controlled mobile phone containing a payment application that is compliant with the Standards. A Mobile Payment Device is differentiated from an Access Device in that a Mobile Payment Device uses an integrated keyboard and screen to access a Card account. (See Card.)

Payment Facilitator

A Merchant registered by an Acquirer to facilitate Transactions on behalf of Sub-merchants.

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 that meets the Corporation's requirements, and that permits a Cardholder to initiate and effect a Transaction for the purchase of products or services sold by such Merchant with a Card in accordance with the Standards.

Principal Member, Principal

A financial institution that is eligible and approved to be a Member pursuant to MasterCard Rule 1.1.2. "Principal" is an alternative term for Principal Member. A Principal Member is also referred to as a Customer.

Program

A Customer's Card issuing program, Merchant acquiring program, or both.

Program Service(s)

Any service described in MasterCard Rule 7.1 that directly or indirectly supports a Program. The Corporation has the sole right in its sole discretion to determine whether a service is a Program Service.

Service Provider

A person that performs Program Service. The Corporation has the sole right in its sole discretion to determine whether a person is 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.

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.

Standards

The Amended and Restated Certificate of Incorporation, Bylaws, MasterCard Rules, and policies, and the operating regulations and procedures of the Corporation, including but not limited to any manuals, guides or bulletins, as may be amended from time to time.

Sub-merchant

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

Third Party Processor (TPP)

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

Transaction

The sale of goods or services by a Merchant to a Cardholder pursuant to acceptance of a Card by the Merchant.

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..... 1-1
1.2 Conflict with Law 1-1
1.3 The Security Contact 1-1

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 MasterCard Rule 3.1.2, unless otherwise specified in the table below. The noncompliance assessment schedule provided in MasterCard Rule 3.1.2 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
2.2	Contracting with Card Registration Companies	C
3.11.3	Standard Wording	B
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.

Chapter 2 Omitted

This chapter has been omitted.

Chapter 3 MasterCard Card and TID Design Standards

This chapter may be of particular interest to Issuers and vendors certified by MasterCard responsible for the design, creation, and control of MasterCard cards. It provides specifications for all consumer and corporate Card Programs worldwide.

3.8 Mobile Payment Devices.....	3-1
3.9 Card Validation Code (CVC)	3-1
3.9.4 Acquirer Requirements for CVC 2	3-1
3.10 Service Codes.....	3-2
3.10.1 Issuer Information	3-2
3.10.2 Acquirer Information.....	3-2
3.10.3 Valid Service Codes	3-3
3.10.4 Additional Service Code Information	3-4
3.11 Transaction Information Documents (TIDs).....	3-5
3.11.1 Formset Contents.....	3-6
3.11.2 Point-of-Sale (POS) Terminal Receipt Contents.....	3-6
3.11.3 Standard Wording.....	3-7
3.11.4 Primary Account Number Truncation and Expiration Date Omission.....	3-8

3.8 Mobile Payment Devices

There is no limitation on the type of account that may co-reside on the same Mobile Payment Device user interface, so long as such accounts are not linked, but rather exist independently and are accessed by a separate and distinct payment application hosted on the same user interface.

The application software and personalization data for a *PayPass* Mobile Payment Device must comply with the applicable technical specifications, as may be published by MasterCard from time to time.

The *PayPass* application must be implemented within a secure IC (the Secure Element [SE]). The SE must be CAST-approved and have received a mobile payment certificate number (MPCN). Issuers may choose a CAST-approved SE (with corresponding MPCN) from the list published on MasterCard OnLine. The Mobile Payment Device itself does not undergo a CAST approval. Prior to issuance of the Mobile Payment Device, the *PayPass* application must also pass the functional and security testing Program, for which a letter of approval will be issued by MasterCard.

For information regarding CAST, refer to the *Compliance Assessment and Security Testing Program* manual. For information regarding a letter of approval, refer to the *Mobile MasterCard PayPass Issuer Implementation Guide*.

Mobile Payment Devices may support *PayPass* functionality. If an Issuer chooses to add this functionality to a Mobile Payment Device, the *PayPass* functionality must comply with the requirements set forth in the Standards, including but not limited to, the technical specifications, and the MasterCard *PayPass* Branding Standards, as may be published by MasterCard from time to time.

3.9 Card Validation Code (CVC)

The CVC is a security feature with components identified elsewhere in this manual. Use of CVCs makes it more difficult for counterfeiters to alter Cards and reuse them for fraudulent purposes.

3.9.4 Acquirer Requirements for CVC 2

When the Merchant provides the indent-printed CVC 2 value, the Acquirer must include the CVC 2 value in DE 48, subelement 92 of the Authorization Request/0100 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.

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

3.10 Service Codes

The service code, a three-digit number that complies with ISO 7813 (Identification Cards—Financial Transaction Cards), 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 EMV chip Cards used in chip Card or hybrid terminals, the 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.

3.10.1 Issuer Information

Currently, MasterCard recommends using service code value 101 (international Card, normal authorization, normal Cardholder verification, no restrictions) for most Card applications. For more information, refer to Table 3.3 in this chapter.

MasterCard Electronic Issuers must encode a value of 2 (positive online authorization required) in position 2 of the service code.

Issuers may use service codes to support issuance of integrated circuit Card (ICC) applications and PIN requirements.

Issuers are strongly recommended to set authorization parameters that decline any magnetic stripe Transaction containing the invalid service code value of 000 for purposes of fraud prevention.

3.10.2 Acquirer Information

Acquirers must ensure that their hybrid POI 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 payment application. The hybrid POI terminal must first attempt to process the Transaction as a chip Transaction; or
- The POI 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.

3.10.3 Valid Service Codes

Table 3.3 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 3.1—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

MasterCard Card and TID Design Standards

3.10 Service Codes

Definition	Position 1	Position 2	Position 3
Normal Cardholder Verification—Goods and services only at Point of Interaction (no cash back)			2
ATM Only, PIN Required			3
PIN Required—Goods and services only at Point of Interaction (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 Service (no cash back)			7

NOTE

In Authorization Release 06.2, support of Purchase of Goods and Services with Cash Back Transactions was mandated for Debit MasterCard® cards. Position 3, values 5 and 7 are not valid values applicable for Debit MasterCard Transactions.

3.10.4 Additional Service Code Information

The following information explains the service code values in Table 3.3.

- Normal authorization is an authorized Transaction according to the established rules governing Transactions at the Point of Interaction.
- 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 Cardholder verification method must be performed in accordance with established rules governing Cardholder verification at the Point of Interaction.
- ICC-related service codes (value of 2 or 6 in position 1) are permitted only on EMV chip Cards containing a MasterCard 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

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.

3.11 Transaction Information Documents (TIDs)

Transaction Information Documents (TIDs) used in interchange Transactions must comply with the Standards set forth in this section.

Below is a list of the types of TIDs discussed in this section:

- Retail sale
- Credit
- Cash disbursement
- Information

NOTE

The Acquirer must retain a copy of the TID for at least 18 months.

If the Merchant uses a manual imprinter, the TID produced is called a formset or slip. For MasterCard formset specifications, refer to [Appendix B](#).

If a Transaction begins at an electronic terminal, the Merchant may substitute a terminal receipt for a formset. Terminal receipts have no prescribed physical specifications but must be numbered sequentially for reference purposes.

A TID must not reflect the following information:

- The PIN, any part of the PIN, or any fill characters representing the PIN
- The CVC 2, which is present in a white panel adjacent to the signature panel of the Card

MasterCard prohibits the recording of PIN data and CVC data in any manner for any purpose.

3.11.1 Formset Contents

Each copy of a retail sale, credit, or cash disbursement formset shall satisfy minimum statutory and regulatory requirements in the jurisdiction in which the slip originates and any applicable regulations, issued by the U.S. Board of Governors of the Federal Reserve System or other regulatory authorities, and shall contain the following:

- In the case of retail sale and credit slips, a space for the description of goods, services, or other things of value sold by the Merchant to the customer and the cost thereof, in sufficient detail to identify the Transaction.
- Adequate spaces for:
 - The customer’s signature
 - Card imprint and the Merchant or bank identification plate imprint
 - Date of the Transaction
 - Authorization number (except on credit slips)
 - Sales clerk’s or teller’s initials or department number
 - Currency conversion field
 - Merchant’s signature on credit slips
 - Description of the positive identification supplied by the Cardholder on cash disbursements and retail sale slips for certain unique Transactions.
- A legend clearly identifying the slip as a retail sale, credit, or cash disbursement and identifying the receiving party of each copy.
- On the customer copy of the formset, the words (in English, local language, or both): “IMPORTANT—retain this copy for your records,” or words to similar effect.
- Such other contents as are not inconsistent with these rules.

MasterCard recommends that each retail sale, credit, and cash disbursement slip bear a means of identifying the Customer that distributed the slip to the Merchant.

3.11.2 Point-of-Sale (POS) Terminal Receipt Contents

Each copy of a Point-of-Sale (POS) Terminal receipt shall satisfy all requirements of applicable law, and shall contain the following information:

- Doing Business As (DBA) Merchant name, city and state, country, or the point of banking location
- Transaction date
- MasterCard account number (refer to section 3.11.4 for details on displaying the MasterCard account number)
- Transaction amount in the original Transaction currency
- Adequate space for the customer's signature, unless the Transaction is completed with a PIN as the Cardholder verification method (CVM) or no CVM (required on Merchant copy only)
- Authorization approval code (except on credit receipts). Optionally, the Acquirer also may print the Transaction certificate, the application cryptogram, or both for EMV chip Card Transactions.
- Merchant's signature on credit receipts only

Each receipt shall clearly identify the Transaction as a retail sale, credit, or cash disbursement.

3.11.3 Standard Wording

MasterCard has developed the following standard wording for use on the interchange copy of the formset. Use the standard wording, which may appear in English, the local language, or both, unless MasterCard has previously granted a variance permitting use of other wording.

- Retail sale slips:

“The Issuer of the Card identified on this item is authorized to pay the amount shown as ‘total’ upon proper presentation. I promise to pay such total (together with any other charges due thereon) subject to and in accordance with the agreement governing the use of such Card.”
- Credit slips:

“I request that the above Cardholder account be credited with the amount shown as ‘total’ because of the return of, or adjustments on, the goods, services, or other items of value described, and authorize the bank to which this credit slip is delivered to charge my account in accordance with my agreement with such bank.”
- Cash disbursement slips:

“I hereby request the Issuer of the Card identified above to pay to bearer the amount shown as ‘total’ hereon. I hereby confirm that I will pay said amount, with any charges due thereon, to said Issuer in accordance with terms of the agreement governing the use of said Card.”
- Information slips:

“Information on this slip relates to the type of Transaction indicated above, and the amount shown hereon as the total should agree with the amount on the receipt provided at the time of the Transaction.”

3.11.4 Primary Account Number Truncation and Expiration Date Omission

The Cardholder and Merchant receipts generated by all electronic POS Terminals, whether attended or unattended, and all printed ATM receipts must omit the Card expiration date. In addition, the Cardholder receipt generated by all electronic POS Terminals, whether attended or unattended, and all printed ATM receipts must reflect only the last four (4) digits of the PAN. All preceding digits of the PAN must be replaced with fill characters, such as “X,” “*,” or “#,” that are neither blank spaces nor numeric characters.

MasterCard strongly recommends that if an electronic POS Terminal generates a Merchant copy of the Cardholder receipt, the Merchant copy should also reflect only the last four (4) digits of the PAN, replacing all preceding digits with fill characters, such as “X,” “*,” or “#,” that are neither blank spaces nor numeric characters.

NOTE

A variation to this rule applicable to ATM transactions appears in section 7.6.1.4 of Chapter 16, “Canada Region,” of the *Cirrus Worldwide Operating Rules* manual.

Chapter 4 Terminal and PIN Security Standards

This chapter may be of particular interest to all MasterCard, Maestro, and Cirrus Issuers and to Acquirers of PIN-based Transactions.

4.1 Personal Identification Numbers (PINs).....	4-1
4.3 PIN Verification	4-1
4.5 PIN Encipherment.....	4-1
4.6 PIN Key Management	4-2
4.6.1 PIN Transmission between Customer Host Systems and the Interchange System.....	4-2
4.6.2 On-behalf Key Management	4-3
4.7 PIN at the Point of Interaction	4-4
4.8 Hybrid Terminal Security Standards.....	4-4
4.8.1 Hybrid Terminals Supporting Offline PIN.....	4-5
4.9 PIN Entry Device Standards	4-5
4.10 Wireless POS Terminals and Internet/Stand-alone IP-enabled POS Terminal Security Standards	4-6
4.11 POS Terminals Using Electronic Signature Capture Technology (ESCT).....	4-7
4.12 Component Authentication	4-7
4.13 Triple DES Migration Standards.....	4-8

4.1 Personal Identification Numbers (PINs)

MasterCard requires Issuers to give their Cardholders a personal identification number (PIN) in conjunction with Card issuance, or offer them the option of receiving a PIN. 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. A PIN also may be used at certain other Point-of-Interaction (POI) terminals.

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

Acquirers 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

The Issuer may use the PIN verification algorithm of its choice.

Refer to “PIN Verification” in the *Authorization Manual*, Chapter 9, “Authorization Services Details” for more information about the MasterCard PIN verification service, in which the MasterCard Worldwide Network performs PIN verification on behalf of Card Issuers, and the two PIN verification methods (IBM 3624 and ABA) that the PIN verification service supports.

Refer to “PIN Generation Verification” in *Single Message System Specifications*, Chapter 6, “Encryption” for more information about PIN verification that the MasterCard Worldwide Network performs directly for Debit MasterCard card and Maestro and Cirrus card Issuers.

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 MasterCard *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 MasterCard purchase 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 OnLine® Publications product.

Table 4.1–PIN Key Management References

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

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.

Terminal and PIN Security Standards

4.7 PIN at the Point of Interaction

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 via the MasterCard OnLine Publications product.

4.7 PIN at the Point of Interaction

MasterCard may authorize the use of a PIN at selected Merchant types, 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 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 EMV chip Transactions.

MasterCard requires Merchants to provide a 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 PIN entry device (PED) as described in section 4.9 of this manual.

Acquirers must control POI 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 Hybrid Terminal Security Standards

A hybrid terminal is a Point-of-Sale (POS) Terminal or ATM that accepts chip Cards in addition to Cards that use magnetic stripe technology.

For interchange operations, MasterCard requires that all hybrid terminals and devices follow these Standards:

- All hybrid terminals and devices must be EMV-compliant.
- All hybrid terminals and devices must be type-approved by MasterCard.
- All hybrid terminals and devices that read and process EMV-compliant payment applications must read and process EMV-compliant MasterCard payment applications.
- All hybrid terminals and devices must be full-grade and Terminal Integration Process (TIP)-approved.
- Acquirers of hybrid terminals and devices must comply with all applicable Standards, including but not limited to the *M/Chip Requirements* manual.
- All offline-capable hybrid terminals and devices must support offline Static Data Authentication (SDA) and offline Dynamic Data Authentication (DDA) as Card authentication methods (CAMs). Offline-capable hybrid terminals and devices undergoing MasterCard certification on or after 1 January 2011 also must support offline Combined Data Authentication (CDA) as a CAM.
- All offline-capable hybrid terminals and devices undergoing MasterCard certification on or after 1 January 2011 must support offline PIN processing as a Cardholder verification method (CVM). This requirement does not apply in Taiwan until 1 January 2013.

4.8.1 Hybrid Terminals Supporting Offline PIN

Hybrid terminals support both magnetic stripe and Europay-MasterCard-Visa (EMV) chip Cards.

All terminals that support offline PIN Transactions must support both clear text and enciphered offline PIN options.

Hybrid terminals must support online dynamic Card authentication methodology (CAM) for all chip-read Transactions.

4.9 PIN Entry Device Standards

Acquirers must ensure that all PEDs that are part of POS Terminals meet the following 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 Payment Card Industry (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.

Terminal and PIN Security Standards

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

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 9564-2 and the appropriate PIN block format as provided in ISO 9564-1.

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 9564-2.

4.10 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 via 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.

4.11 POS Terminals Using Electronic Signature Capture Technology (ESCT)

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

- That 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.
- That 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.
- That 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 use of ESCT if it identifies inadequate controls.

4.12 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.

4.13 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.

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	5-1
5.1.1 Point-of-Interaction (POI) Card Retention	5-1
5.1.1.1 Returning Recovered Cards	5-1
5.1.1.2 Returning Counterfeit Cards	5-1
5.1.1.3 Liability for Loss, Costs, and Damages	5-2

5.1 Card Recovery and Return

5.1.1 Point-of-Interaction (POI) Card Retention

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.

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 Business Forms section of MasterCard OnLine®.

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 MasterCard bank identification number (BIN) present in the Account Information Area.
- The Member ID imprinted in the Card Source Identification area on the back of the Card.

Card Recovery and Return Standards

5.1 Card Recovery and Return

In the absence of a BIN or Member ID, the Issuer may be identified by any other means, including the bank name printed on the front or back of the Card or the magnetic stripe. If the Issuer is still unidentifiable, return the Card to the MasterCard vice president of the Security and Risk Services Department.

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 Fraud Loss Control Program Standards 6-1
 - 6.2.2 Acquirer Fraud Loss Control Programs..... 6-1
- 6.3 Counterfeit Card Fraud Loss Control Standards 6-1
 - 6.3.1 Counterfeit Card Notification..... 6-1
 - 6.3.1.2 Notification by Acquirer 6-2
 - 6.3.1.3 Failure to Give Notice 6-2

6.2 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's fraud loss control program must meet 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.

To comply with the fraud loss control Standards, Acquirers also must transmit complete and unaltered data in all Card-read authorization request messages, and also CVC 2 for all CNP and voice-authorized Transactions.

Additionally, Acquirers with high fraud levels must:

- Install “read and display” terminals in areas determined to be at high risk for fraud or counterfeit activity, or
- Install EMV chip terminals

6.3 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, Issuers are required to incorporate the Card security features described in [Chapter 3](#) on all Cards, and Acquirers must transmit full magnetic stripe or chip data on all POI Card-read 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 Security and Risk Services representative and the Issuer by phone, e-mail, 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.

Chapter 7 Merchant Screening and Monitoring Standards

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

7.1 Screening New Merchants.....	7-1
7.1.1 Evidence of Compliance with Screening Procedures	7-1
7.1.2 Retention of Investigative Records	7-2
7.1.3 Assessments for Noncompliance with Screening Procedures.....	7-3
7.1.4 Screening Limitations	7-3
7.2 Ongoing Merchant Monitoring and Education.....	7-3
7.2.1 Merchant Monitoring.....	7-4
7.2.2 Additional Requirements for Certain Merchant Categories.....	7-4
7.2.3 Merchant Education	7-4

7.1 Screening New Merchants

Before signing a Merchant Agreement, each Acquirer must verify that the Merchant from which it intends to acquire Transactions is a valid business, as described in MasterCard Rule 5.1.1, Verify Bona Fide Business Operation. Such verification must include at least all of the following:

- Credit check, background investigations, and reference checks of the Merchant.

If the credit check of the Merchant raises questions, the Acquirer also should conduct a credit check of:

- The owner, if the Merchant is a sole proprietor; or
 - The partners, if the Merchant is a partnership; or
 - The principal shareholders, if the Merchant is a corporation.
- Inspection of the premises and records to ensure that the Merchant has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit and other capabilities to conduct the business. If the Merchant has more than one outlet, the Acquirer must inspect at least one outlet from which it will acquire Transactions.
 - Inquiry to the MasterCard Member Alert to Control (High-risk) Merchants (MATCH™) system.
 - Investigation of the Merchant's previous Merchant Agreements.

NOTE

No Customer is exempt from participation in the MATCH system.

An Acquirer is not required to conduct a credit check of a public or private company that has annual sales revenue in excess of USD 50 million (or the foreign currency equivalent), provided the Acquirer reviews, and finds satisfactory for purposes of the acquiring being considered, the most recent annual report of the Merchant, including audited financial statements. A private company that does not have a recent audited financial statement is subject to a credit check and inspection even if its annual sales revenue exceeds USD 50 million.

7.1.1 Evidence of Compliance with Screening Procedures

As evidence that the Acquirer is in compliance with the screening requirements set forth in this chapter, MasterCard requires, at a minimum, the following information:

Merchant Screening and Monitoring Standards

7.1 Screening New Merchants

- A 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
- A written inspection report of the Merchant premises, including verification by the inspector that the Merchant is conducting business in accordance with its agreement; that the Merchant, if required, has a valid license or permit; and that staff and stock levels are adequate
- Proof of the Acquirer's inquiry into the MATCH system, including a copy of the inquiry record
- A statement from the Merchant about previous Merchant Agreements, including the name(s) of the entity(ies) where the Merchant has or had the agreement(s) and the reason(s) for terminating the agreement(s), if applicable

7.1.2 Retention of Investigative Records

The Acquirer must retain all records concerning the investigation of any Merchant with which it has entered into a Merchant Agreement for a minimum of two years after the date that the agreement is terminated. MasterCard recommends that Acquirers retain the following records as a best practice:

- Signed Merchant Agreement
- Previous Merchant statements
- Corporate or personal banking statements
- Credit reports
- Site inspection report, to include photographs of premises, inventory verification, and the name and signature of the inspector of record
- Merchant certificate of incorporation, licenses, or permits
- Verification of references, including personal, business, or financial
- Verification of the authenticity of the supplier relationship for the goods or services (invoice records) that the Merchant is offering the Cardholder for sale
- Date-stamped MATCH inquiry records
- Date-stamped MATCH addition record
- All Customer correspondence with the Merchant
- All correspondence relating to Issuer, Cardholder, or law enforcement inquiries concerning the Merchant 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 of the *MasterCard Rules* manual for more information about Service Providers.

NOTE

MasterCard recommends that Acquirers retain these records to verify compliance in the event of an audit, according to section 7.1.3.

7.1.3 Assessments for Noncompliance with Screening Procedures

MasterCard may audit an Acquirer for compliance with Merchant screening procedures, 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 Merchant screening procedures.

If MasterCard determines that an Acquirer has not complied with Merchant 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 before signing a Merchant Agreement may result in an assessment of up to USD 5,000 for each instance of noncompliance.

7.1.4 Screening Limitations

Screening Merchants, as required by the Standards, does not relieve a Customer from the responsibility of following good commercial banking practices. The review of an annual report or an audited statement, for example, might suggest the need for further inquiry.

7.2 Ongoing Merchant Monitoring and Education

Once a Merchant Agreement is established, an Acquirer must institute an ongoing relationship of fraud prevention, including an education process consisting of periodic visits to Merchants, distribution of related educational literature, and participation in Merchant seminars.

Merchant Screening and Monitoring Standards

7.2 Ongoing Merchant Monitoring and Education

The Acquirer regularly, as reasonably appropriate in light of all circumstances, must review and monitor the Merchant's Web site(s) and business activities to confirm and to reconfirm regularly that any Merchant activity related to or using a Mark is conducted in a legal and ethical manner and in full compliance with the Standards.

As a best practice, MasterCard recommends that Acquirers use a Web site monitoring solution to review their electronic commerce (e-commerce) Merchants' activity to avoid processing illegal or brand-damaging Transactions.

7.2.1 Merchant Monitoring

An Acquirer must monitor each of its Merchant's Transaction activity (sales, credits, and chargebacks) in an effort to deter fraud. Monitoring must focus on changes in activity over time, activity inconsistent with the Merchant's business, or exceptional activity relating to the number of Transactions and Transaction amounts outside the normal fluctuation related to seasonal sales. Specifically, ongoing monitoring includes, but is not limited to, the Acquirer fraud loss controls relating to Merchant deposit (including credits) and authorization activity described in [section 6.2.2](#).

7.2.2 Additional Requirements for Certain Merchant Categories

Acquirers of telecom Merchants, electronic commerce adult content (videotext) Merchants, non-face-to-face gambling Merchants, non-face-to-face prescription drug and tobacco Merchants, state lottery Merchants (U.S. region only), and Merchants reported under the Excessive Chargeback Program must comply with the Merchant registration and monitoring requirements of the MasterCard Registration Program (MRP) for each such Merchant, as described in [Chapter 9](#).

7.2.3 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 presentation of the Transaction to the Acquirer, and proper handling pursuant to Card capture requests. Customers must thoroughly review with Merchants the Standards against the presentation 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.

Chapter 8 Merchant Fraud Control Programs

This chapter may be of particular interest to Customer personnel responsible for identifying Merchant violations.

8.1 Presenting Valid Transactions.....	8-1
8.1.1 Notifying MasterCard—Acquirer Responsibilities	8-1
8.1.2 Notifying MasterCard—Issuer Responsibilities	8-1
8.1.3 MasterCard Audit.....	8-1
8.1.3.1 Initiation of MasterCard Audit	8-2
8.1.3.2 Information Required by MasterCard	8-2
8.1.3.3 Notification to Customers of Chargeback Period.....	8-3
8.2 Global Merchant Audit Program	8-3
8.2.1 Acquirer Responsibilities	8-4
8.2.2 Tier 3 Special Merchant Audit	8-5
8.2.3 Chargeback Responsibility	8-7
8.2.4 Exclusion from the Global Merchant Audit Program.....	8-8
8.2.4.1 Systematic Exclusions	8-8
8.2.4.2 Exclusion after GMAP Identification.....	8-9
8.2.5 Notification of Merchant Identification.....	8-10
8.2.5.1 Distribution of Reports	8-10
8.2.6 Merchant Online Status Tracking (MOST) System.....	8-11
8.2.6.1 MOST Mandate.....	8-11
8.2.6.2 MOST Registration.....	8-12
8.3 Excessive Chargeback Program.....	8-13
8.3.1 Definitions.....	8-13
8.3.2 Reporting Requirements.....	8-13
8.3.2.1 Chargeback-Monitored Merchant Reporting Requirements	8-14
8.3.2.1.1 CMM Report Contents.....	8-14
8.3.2.1.2 Late CMM Report Submission Assessment.....	8-14
8.3.2.2 Excessive Chargeback Merchant Reporting Requirements	8-14
8.3.2.2.1 ECM Report Contents	8-15
8.3.2.2.2 Late ECM Report Submission Assessment.....	8-15
8.3.3 Assessments	8-15
8.3.3.1 ECP Assessment Calculation.....	8-15
8.3.4 Issuer Reimbursement	8-17
8.4 Cardholder-Merchant Collusion (CMC) Program.....	8-17

Merchant Fraud Control Programs

8.4.1 Issuer Notification to MasterCard	8-19
8.4.2 MasterCard Audit.....	8-20
8.4.3 Acquirer Investigation and Response	8-20
8.4.3.1 Merchant Termination	8-21
8.4.4 MasterCard Notification to Issuers.....	8-21
8.4.5 Issuer Obligation to Assist in MasterCard Audit	8-21
8.4.6 MasterCard Evaluation.....	8-22
8.4.6.1 MasterCard Post-Audit Procedures	8-22
8.4.7 Issuer Post-Audit Reporting Procedures	8-22
8.4.8 Issuer Recovery Claim Filing Process	8-23
8.4.8.1 Form for Issuer Recovery Claim Filing Under the CMC Program	8-23
8.4.8.2 Required Acknowledgement	8-25

8.1 Presenting Valid Transactions

A Merchant must present to its Acquirer only valid Transactions between itself and a bona fide Cardholder.

A Merchant must not present a Transaction that it knows or should have known to be fraudulent or not authorized by the Cardholder, or authorized by a Cardholder who is in collusion with the Merchant for a fraudulent purpose. Within the scope of this rule, the Merchant is responsible for the actions of its employees.

8.1.1 Notifying MasterCard—Acquirer Responsibilities

An Acquirer must immediately notify Merchant Fraud Control staff in writing when, in regard to a Merchant with whom it has entered into a Merchant Agreement:

- The Acquirer may have reason to believe that the Merchant is engaging in collusive or otherwise fraudulent or inappropriate activity, **or**
- The Acquirer determines that the Merchant's ratio of chargebacks, credits to sales exceeds criteria established by MasterCard.

An Acquirer must accept chargebacks for all fraudulent Transactions that took place during the period when the Merchant was in violation of MasterCard Rule 5.9.1, Valid Transactions.

Moreover, if an Acquirer fails to identify and declare a Merchant in violation of the Standard, MasterCard may do so after an audit of the Customer's Merchant file and records.

8.1.2 Notifying MasterCard—Issuer Responsibilities

If an Issuer becomes aware of any Merchant in violation of MasterCard Rule 5.9.1, through Cardholder complaints or otherwise, the Issuer immediately must notify Merchant Fraud Control staff at the address and fax number provided in [Appendix C](#).

8.1.3 MasterCard Audit

MasterCard, in its sole discretion, and either itself or by use of a third party, may conduct an audit of an Acquirer's Merchant files and records to determine whether the Merchant is a "questionable Merchant." Merchant Fraud Control staff will notify the Acquirer of a decision to conduct such an audit. An Acquirer and its Merchants must cooperate fully. During the audit, MasterCard may list the Merchant on the Member Alert to Control High-risk (Merchants) (MATCH™) system under MATCH reason code 00 (Questionable Merchant).

Merchant Fraud Control Programs

8.1 Presenting Valid Transactions

In the course of the audit, staff will develop allegations from any available sources, including, but not limited to, internal studies, analyses, Customer input and complaints, and from information derived from compliance actions regarding activities by Merchants which would raise serious concerns as to whether such Merchants have caused to be entered into interchange Transactions which the Merchants knew or should have known were fraudulent or resulted in excessive costs to the industry.

It is the obligation of the Acquirer to monitor each Merchant closely.

MasterCard may assess the Acquirer for costs and expenses incurred related to the audit.

8.1.3.1 Initiation of MasterCard Audit

If MasterCard suspects that a Merchant may be in violation of MasterCard Rule 5.9.1, MasterCard will send a letter to the Security Contact listed in the Member Information tool. The Security Contact is responsible for distributing the letter to the person responsible for the Acquirer's Merchant audit programs. The letter explains why MasterCard is conducting the audit and assessments associated with violations of MasterCard Rule 5.9.1. Customers must return the requested information to Merchant Fraud Control for each Merchant listed in the letter within 30 calendar days of the date of the cover letter.

8.1.3.2 Information Required by MasterCard

The following is a list of some of the items that MasterCard may require Acquirers to provide during the course of an audit, initiated by MasterCard to determine whether an Acquirer's Merchant was in violation of MasterCard Rule 5.9.1:

1. A detailed statement of facts explaining whether, when, and how the Customer became aware of fraudulent activity or chargeback or customer service issues, the steps taken by the Customer to control the occurrence of fraud, and the circumstances surrounding the Merchant's termination.
2. All internal documents about the opening and signing of the Merchant including its application, Merchant Agreement, credit report, and certified site inspection report. (The Acquirer should include the Merchant's opening and closing dates.)
3. All internal Customer documents regarding the due diligence procedures followed before signing the Merchant, including background checks of the company and its principals, and the telephone logs for trade and bank references that the Customer verified during the due diligence procedure.
4. Internal reports, where applicable, confirming inquiry by the Customer into the MATCH system before signing the Merchant and, if applicable, input of the Merchant to the MATCH system database within five business days after its decision to close the Merchant as specified in these rules.

If a Service Provider of an Acquirer facilitates the signing of a Merchant, the Service Provider must include the due diligence documents.

Additionally, if an Acquirer's Service Provider assisted in the signing of the Merchant, the Customer must provide all Service Provider due diligence documents regarding the representative that signed the Merchant.

Staff will establish an audit (review) period for which the Acquirer must provide the following supporting documentation:

1. Authorization logs for the Merchant.
2. If requested to do so, the Acquirer must provide a monthly breakdown of chargeback and credits by count, amount, and Issuer bank identification number (BIN) for the suspected violation period, as specified by MasterCard.
3. A complete record of the Merchant sales volume, including the number of Transactions at the location, for the period for which MasterCard requests the authorization logs. Customers outside the U.S. region that do not report their local fraud to the System to Avoid Fraud Effectively (SAFE) may not include local sales in the Merchant's sales volume.

MasterCard may require the Customer to provide additional information deemed relevant to the audit. In the event that an Acquirer refuses to disclose information requested by MasterCard, MasterCard may, in its sole discretion for the purpose of the audit, presume that the information would not be favorable to the Acquirer and declare the Merchant in violation of MasterCard Rule 5.9.1.

8.1.3.3 Notification to Customers of Chargeback Period

If MasterCard determines that a Merchant is a questionable Merchant, MasterCard will publish a *Global Security Bulletin* identifying the Merchant and specifying the appropriate chargeback period. The Issuer has 120 calendar days from the date of the *Global Security Bulletin* to charge back Transactions to the Acquirer (using IPM message reason code 4849—Questionable Merchant Activity).

In the case of Transactions occurring after the date of the *Global Security Bulletin*, but within the dates specified, the Issuer has 120 calendar days from the date of the Transaction to charge back the Transactions. The Issuer must include the number of the *Global Security Bulletin* (for example, "Global Security Bulletin No. XX") in the Data Record Text (Data Element 72) when processing the chargeback.

8.2 Global Merchant Audit Program

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

Merchant Fraud Control Programs

8.2 Global Merchant Audit Program

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

A Merchant location is classified in the following GMAP tier...	If in any calendar month, the Merchant location meets the following fraud criteria...
Tier 1—Informational Fraud Alert	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Five fraudulent Transactions• At least USD 5,000 in fraudulent Transactions• A fraud-to-sales dollar volume ratio minimum of 8%

If a 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 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 via 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 via 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 MasterCard Rule 5.9.1 (a “questionable Merchant”), as described in [section 8.1.3](#), 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 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

Merchant Fraud Control Programs

8.2 Global Merchant Audit Program

month in which the Merchant was first identified in GMAP. Fraudulent Transactions reported to 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

February	Month 1 March	Month 2 April	Month 3 May	Month 4 June	Month 5 July	Month 6 August
30-DAY RESPONSE PERIOD 15 February to 15 March				After the implementation of the fraud control action plan, GMAP reviews SAFE reported fraudulent transactions for Months 4 and 5, and incrementally thereafter until a rolling six months is resumed. (For example, in Month 6, GMAP reviews fraud in Months 4 and 5.)		
90-DAY ACTION PERIOD 1 March to 30 May						
<p>2 February GMAP identifies a merchant in Tier 3. MasterCard conducts a review of fraud criteria.</p> <p>15 February By this date, MasterCard is expected to have notified the acquirer that a Tier 3 special merchant audit has been initiated.</p>	<p>15 March The end of the 30-day response period. The acquirer must respond in MOST by either indicating that the merchant has been terminated or by completing the online questionnaire through MOST.</p> <p>30 March By this date, MasterCard is expected to have determined whether further action is required, and if so, provide a fraud control action plan.</p>	<p>31 March to 29 May The acquirer implements the fraud control action plan.</p>	<p>30 May By this date, the acquirer must have implemented the fraud control action plan at the merchant location. MasterCard requires the acquirer to confirm successful implementation.</p>	<p>Fraud reported to SAFE becomes eligible for GMAP identification.</p>	<p>Fraud reported to SAFE becomes eligible for GMAP identification.</p>	<p>Merchant is eligible for GMAP identification.</p>
<p>CHARGEBACK LIABILITY PERIOD MasterCard may list the merchant in a <i>Global Security Bulletin</i>, thereby alerting issuers that the acquirer will be responsible for chargebacks. The six-month period will be from 1 June through 30 November.</p>						

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 *Global Security Bulletin*.

When MasterCard lists the Acquirer and Merchant information in a *Global Security Bulletin*, 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 Present¹ 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 the *SAFE Products User Guide*). 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 *Global Security Bulletin*, the Issuer may not use message reason code 4849—Questionable Merchant Activity, in any of the following situations:

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.

Merchant Fraud Control Programs

8.2 Global Merchant Audit Program

- 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* global liability shift for 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 UCAF data for that Transaction, 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 Point-of-Interaction (POI) 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.

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.

Merchant Fraud Control Programs

8.2 Global Merchant Audit Program

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 the GMAP. If an Acquirer does not receive an automated notification, it is the Acquirer's responsibility to obtain this information through MasterCard OnLine®.

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 OnLine 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 via 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 OnLine 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 via MOST and then chooses to submit supporting documentation via 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 4,000.

8.2.6.2 MOST Registration

To use MOST, a user must be licensed for each acquiring Member ID/ICA number at a child level, regardless of a parent/child relationship. Each user access request to the MOST system first is submitted by the requester via the Product Catalog on MasterCard OnLine. The request then is submitted to the Customer's MasterCard Online Administration Tool (MAT) administrator for approval. The MAT administrator is responsible for approving authorization for a Customer user or processor to use the MOST system for that Customer's specified Member IDs/ICA numbers. After the access request is approved by the MAT administrator, the request automatically is sent to MasterCard for processing.

MasterCard will decline requests for access to the MOST system that are not complete, accurate, or approved by the MAT administrator for each Member ID/ICA number for which the user is requesting MOST access. MasterCard staff 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 access. When MasterCard declines a user access request, the user must resubmit a subsequent online MOST product registration request to the Customer's MAT administrator for approval. Once approved by the MAT administrator, the request automatically will be routed to MasterCard for processing. To register for MOST, follow the steps in Table 8.2.

Table 8.2—Registering for MOST

Step	Action
1.	Go to www.mastercardonline.com .
2.	Login to MasterCard OnLine by entering your User ID and Security Information .
3.	From the Products menu on the left of your screen, click Order Products to open the MasterCard OnLine—Product Catalog window.
4.	From the Browse Catalog tab, select the Product Name option button.
5.	Search the list alphabetically, or to filter your search, type MOST into the Search box and click Go .
6.	Click MOST .
7.	Click Subscribe Now located in the lower half of the window.
8.	Complete the request form and submit for processing.

NOTE

To update an existing MOST License, follow the navigation instructions above, and click Update Subscription instead of Subscribe Now.

For additional assistance with registering for the MOST online system, contact the Customer Operations Services team using contact information provided in [section C.6](#) of Appendix C.

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 Merchant has exceeded or is likely to exceed monthly chargeback thresholds.

8.3.1 Definitions

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

Merchant	A Merchant is defined as any distinct Merchant location, whether a Merchant's physical location or a Merchant's Internet site or uniform resource locator (URL) that is uniquely identified 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.)
Chargeback-Monitored Merchant (CMM)	A CMM is a Merchant that has a CTR in excess of 50 basis points and at least 50 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 100 basis points and at least 50 chargebacks in each month. This designation is maintained until the ECM's CTR is below 100 basis points for two consecutive months.

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, and 7.2.3 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 a CMM or ECM the reporting fees set forth in sections 8.3.2.1.2 and 8.3.2.2.2.

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 Merchant. MasterCard will assess the Acquirer a reporting fee of USD 50 for each CMM report submitted.

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 the Acquirer or 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 100 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 Merchant. MasterCard will assess the Acquirer a reporting fee of USD 300 for each ECM report submitted.

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 description of the Acquirer's chargeback controls in place to monitor the ECM's activities
- An evaluation of the practices that caused the ECM to exceed the ECP Standard
- An Acquirer action plan to reduce the ECM's CTR
- An electronic file that contains chargeback Transaction detail 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

MasterCard will assess the Acquirer a reporting fee of USD 300 for each ECM report submitted.

8.3.2.2.2 Late ECM Report Submission Assessment

If the Acquirer or 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 per day thereafter until the delinquent ECM report is submitted.

8.3.3 Assessments

In addition to any applicable assessments for CMM reports, 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 100 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.

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 100 basis points (which may also be expressed as 1% or 0.01).

Merchant Fraud Control Programs

8.3 Excessive Chargeback Program

2. From the total number of chargebacks in the above CTR calculation, subtract the number of chargebacks that account for the first 100 basis points of the CTR. (This amount is equivalent to one percent of the number of monthly sales Transactions used to calculate the CTR.) The result is the number of chargebacks above the threshold of 100 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 100 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 100 basis points or one 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 Transaction	95,665	95,460	95,561	95,867	95,255	95,889	95,758
Chargebacks	720	1003	1301	1256	1175	923	824
CTR in basis points	—	105	136	131	123	97	86

February and March are the trigger months, as these are two consecutive months where the CTR exceeded 100 basis points. At the end of July, Merchant ABC was no longer an ECM as its CTR was below 100 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 = $1,256/95,561 = 0.01314$ or 131 basis points (rounded)
- The number of chargebacks in excess of the 100 basis points is determined by subtracting one percent of the March sales Transactions from the number of April chargebacks. One percent of the March sales Transactions ($95,561 \times 0.01$) is 956. $1256 - 956 = 300$ chargebacks
- The Issuer reimbursement for April is $300 \times \text{USD } 25 = \text{USD } 7,500$
- The violation assessment is $(\text{USD } 7,500 \times 131)/100$ or $982,500/100 = \text{USD } 9,825$

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 8,650	USD 11,764	USD 20,414
April	USD 7,500	USD 9,825	USD 17,325
May	USD 5,400	USD 6,642	USD 12,042
June	0	0	0
July	0	0	0
Total	USD 21,550	USD 28,231	USD 49,781

8.3.4 Issuer Reimbursement

MasterCard will remit Issuer reimbursement fees to Issuers through the MCBS. Actual reimbursements will vary depending on the extent and duration of the violation and the number of chargebacks processed by each Issuer, and will be paid out of the amounts collected for the Issuer reimbursement fees described in section 8.3.3.1 on a pro rata basis.

8.4 Cardholder-Merchant Collusion (CMC) Program

The Cardholder-Merchant Collusion (CMC) Program permits an Issuer to file a claim against the Acquirer associated with an identified fully collusive Merchant, and to seek partial recovery (the lesser of [i] one-half of the credit limit in effect at the time that the Issuer closed the Cardholder bust-out account, or [ii] one-half of the actual amount of fraud losses) for fraud losses attributable to Transactions on Cardholder bust-out accounts conducted at a fully collusive Merchant. The recovery eligibility and applicable conditions, procedures, and limits are described in this section.

NOTE

Any Customer that elects to participate in any manner in the CMC Program agrees to comply at all times with all applicable laws and regulations, including those that in any manner govern the collection, storage, and use of personal and Transaction information and the extension of credit. The Customer further agrees that any such participation will be deemed an act that gives rise to an obligation of the Customer to protect, indemnify, and hold harmless MasterCard and those others specified in MasterCard Rule 3.3, Indemnity and Limitation of Liability.

For the purposes of the CMC Program, a **fully collusive Merchant** is defined as a Merchant that:

Merchant Fraud Control Programs

8.4 Cardholder-Merchant Collusion (CMC) Program

- Presents Transactions authorized by a Cardholder that is in collusion with the Merchant for a fraudulent intent and in violation of MasterCard Rule 5.9.1, Valid Transactions, and
- Meets all of the following criteria:
 - The Merchant submits at least USD 5,000 in Transaction volume in any one month, and
 - At least 50 percent of the Merchant’s Transaction volume results from collusive Transactions, and
 - The Merchant has processed Transactions for at least 30 calendar days.

MasterCard may determine that the “fully collusive Merchant” definition has been satisfied at the individual Issuer’s level or at the total MasterCard system level.

A **Cardholder bust-out account** is defined as an account to which all of the following conditions apply:

1. A balance that is over the account’s credit limit, and
2. A returned payment, followed by Cardholder attempts to make additional purchases or cash advances or the proactive canceling of the account by the Issuer before the attempted deposit of a check that the Issuer returns unpaid (for example, a not-sufficiently-funded [NSF] check or a check drawn on a closed account), and
3. An unusual pattern of purchase activity at a particular Merchant location (for example, a Cardholder who typically makes an occasional purchase of electronic goods suddenly makes multiple purchases at a particular electronic store), and
4. At least one of the following situations exists:
 - a. The account is linked to one or more other Cardholder bust-out accounts (See the **Note** at the end of this section for a description of linked accounts.)
 - b. When the Cardholder established the account, the Cardholder credit history records showed limited credit experience (“thin file”) and the credit report may have indicated frequent inquiries to credit bureaus
 - c. Regular Cardholder requests for credit limit increases (for example, a Cardholder makes requests for substantial credit increases within a short time period)
 - d. Cardholder requests for additional authorized users for the account
 - e. Use of balance transfers and convenience checks
 - f. Frequent balance inquiries, “open-to-buy” queries, or both
 - g. No mortgage loan on file

- h. Unfamiliar or “generic” employer information, employment information, or both (for example, a Cardholder provided no specific employer name and employment dates)
- i. Suspicious residence address (for example, a Cardholder provided a Private Mail Box [PMB] address as the residence address)

Or

The Issuer has closed the account, either because it was linked (see the **Note** at the end of this section) to one or more Cardholder bust-out accounts or as a result of the Issuer’s proactive fraud loss control program strategy, and at least one of the conditions (b) through (i) of item 4 in section 8.4 exists.

Or

The Issuer has closed the account because it is linked to another Merchant that MasterCard has determined to be a fully collusive Merchant.

NOTE

A Cardholder account is linked to one or more other accounts by a common social security number (SSN) or other government-issued identification number, address, phone number, name, authorized users, or demand deposit account number. A link also may be detected if multiple accounts transact at the same suspected collusive Merchant.

8.4.1 Issuer Notification to MasterCard

If an Issuer believes that a Merchant is a fully collusive Merchant engaging in Transactions on a Cardholder bust-out account, the Issuer must notify MasterCard via e-mail at bustouts@mastercard.com within three calendar days of having such reason to believe. Transactions that occurred up to 180 calendar days before the date of the Issuer’s initial notification may qualify as eligible for recovery under the CMC Program.

In the notification, the Issuer must provide the basis for the Issuer’s reason to believe that the Merchant is a fully collusive Merchant, supported by all of the following information:

Merchant Fraud Control Programs

8.4 Cardholder-Merchant Collusion (CMC) Program

- Issuer name and Member ID
- Acquirer name and Member ID
- Merchant name and address (city, state or province, and country)
- Total number of Transactions processed at the Merchant
- Total dollar volume of Issuer losses at the Merchant
- Percentage of collusive Transactions attributed to Cardholder bust-out accounts
- Details of each Issuer-confirmed collusive Transaction, including Cardholder account number, Transaction date and time, and Transaction amount in U.S. dollars
- A report of the Issuer's investigative findings concerning the Merchant
- Complete details of the Issuer's contacts with the Acquirer, if any, concerning the Merchant
- Complete details of the Issuer's knowledge of law enforcement involvement
- Complete details of the Issuer's tracking system (procedures for NSF checks, credit report monitoring, and similar measures)

The Issuer must submit the notification, including all documentation, via e-mail to bustouts@mastercard.com.

8.4.2 MasterCard Audit

Upon receipt of the Issuer notification and at its sole discretion, MasterCard may initiate an audit of the Acquirer's records to determine whether the identified Merchant is a fully collusive Merchant. At the initiation of an audit, MasterCard will notify, via e-mail, certified mail, or fax, the Security Contact of each known Acquirer of the Merchant. MasterCard may list the suspected collusive Merchant in MATCH™ using MATCH reason code 00 (Questionable Merchant) for the duration of the audit.

8.4.3 Acquirer Investigation and Response

Within 15 calendar days from the date of the MasterCard notification, the Acquirer must:

- Investigate the identified Merchant, and
- Submit to MasterCard the documentation listed in [section 8.1.3.2](#), “Information Required by MasterCard,” of this manual, and
- Provide a record of all Transaction activity at the identified Merchant, including the Transaction amounts, dates and times, and affected account numbers, for the 180-calendar-day period preceding the date of initial Issuer notification to MasterCard (MasterCard will provide to the Acquirer the reporting parameters, including the date of initial Issuer notification to MasterCard), and
- Provide such additional information as MasterCard may request.

The Acquirer must submit all documentation and records via certified mail or fax to Merchant Fraud Control as provided in [section C.7 of Appendix C](#), or via e-mail to bustouts@mastercard.com.

8.4.3.1 Merchant Termination

If the Acquirer determines that the Merchant is a fully collusive Merchant and terminates the Merchant Agreement for that reason, the Acquirer must add the Merchant to MATCH using MATCH reason code 11 (Merchant Collusion) within five calendar days of the decision to terminate the Merchant.

8.4.4 MasterCard Notification to Issuers

MasterCard will notify Issuers whose accounts are believed to have been used in Transactions at the Merchant being audited within seven calendar days from the date of receiving the initial Issuer notification. The MasterCard notification to the affected Issuers will use the subject heading “CMC Program Notification—Immediate Action Required.”

Notification will occur via the MasterCard Alerts E-mail Notification Service, or if an Issuer is not a licensed MasterCard Alerts user, then via fax to the Issuer’s Security Contact listed in the Member Information tool. In the notification, MasterCard will provide the Merchant name, city, and state, province, or country.

8.4.5 Issuer Obligation to Assist in MasterCard Audit

Within 30 calendar days of the MasterCard notification, an affected Issuer must provide to MasterCard the documentation described in [section 8.4.1](#) of this manual, using reporting parameters provided by MasterCard in its notification. All reported Transactions must have taken place with the Merchant identified as being the subject of the MasterCard audit. Collusive Transactions on the same account but at different Merchant locations are treated as separate events and must not be included in the documentation for the Merchant that is the subject of the MasterCard audit.

8.4.6 MasterCard Evaluation

MasterCard will determine whether to declare the audited Merchant a fully collusive Merchant.

If an Acquirer becomes aware that it is acquiring for a fully collusive Merchant, the Acquirer must notify MasterCard promptly.

8.4.6.1 MasterCard Post-Audit Procedures

If MasterCard determines that the Merchant **is** a fully collusive Merchant, MasterCard will:

- Notify the Merchant's Acquirer in writing, and
- Identify the Merchant as a fully collusive Merchant in a *Global Security Bulletin*, and
- Modify the Merchant's MATCH record to reflect a reason code change from 00 (Questionable Merchant) to 23 (Merchant Collusion).

If the Acquirer has terminated the Merchant, the Acquirer is required to identify the Merchant in MATCH with reason code 11 (Merchant Collusion).

If the Acquirer continues to acquire from the Merchant after MasterCard declares the Merchant a fully collusive Merchant, the Acquirer must accept liability for chargebacks with message reason code 4849—Questionable Merchant Activity for all fraudulent Transactions reported to SAFE at the identified Merchant location, for a period of at least one year following publication of the *Global Security Bulletin* listing that Merchant.

8.4.7 Issuer Post-Audit Reporting Procedures

To be eligible to file a claim seeking recovery in accordance with the CMC Program, an Issuer must:

- Provide to MasterCard all of the information listed in [section 8.4.1](#), either unprompted or in full cooperation with a MasterCard audit as required by [section 8.4.5](#), and
- Report all Cardholder bust-out account fraud Transactions at the fully collusive Merchant identified in a *Global Security Bulletin* within 120 calendar days of the date of the *Global Security Bulletin*, and
- Remain compliant with such other requirements as set forth in these CMC Program Standards.

Issuers must report to SAFE using fraud type code 51 (Bust-out Collusive Merchant) the aggregate amount of all such Transactions that occurred no more than 180 calendar days before the initial Issuer notification date given in the *Global Security Bulletin*.

8.4.8 Issuer Recovery Claim Filing Process

Within 120 calendar days of the date of the *Global Security Bulletin*, and subject to the completion of the requirements described in these CMC Program Standards, an Issuer may file a claim to request partial recovery of fraud losses (the lesser of [i] one half of the credit limit in effect at the time that the Issuer closed the Cardholder bust-out account or [ii] one half of the actual amount of fraud losses) attributable to Transactions on a Cardholder bust-out account at the fully collusive Merchant. Such Transactions must have occurred at the fully collusive Merchant no more than 180 calendar days before the initial Issuer notification date published in the *Global Security Bulletin*, and no later than the publication date of the *Global Security Bulletin*.

MasterCard will not permit Issuers to file a recovery claim for any Transaction:

- Processed at a Merchant other than those listed in the *Global Security Bulletin*, or
- That took place after the *Global Security Bulletin's* date of publication, or
- Not reported to MasterCard via SAFE OnLine as described in [section 8.4.7](#) of this manual, or
- For which the Issuer received recovery via 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 accepting an Issuer's claim for review and consideration. MasterCard, at its sole discretion, may accept, reduce, or reject claims.

In addition, MasterCard will not pay claims in excess of the amount collected from the Acquirer(s) for that purpose. MasterCard will process Issuer recovery claims via the MasterCard Consolidated Billing System (MCBS).

An Issuer must submit a recovery claim under the CMC Program via certified mail or fax to Merchant Fraud Control at the address and fax number provided in [section C.7 of Appendix C](#), using the form described in [section 8.4.8.1](#) below.

8.4.8.1 Form for Issuer Recovery Claim Filing Under the CMC Program

When filing a recovery claim for Cardholder bust-out Transactions at fully collusive Merchants, Issuers must submit a letter, on letterhead and signed by the Principal Contact, that incorporates the following information:

Merchant Fraud Control Programs

8.4 Cardholder-Merchant Collusion (CMC) Program

- Issuer name and Member ID
- Acquirer name and Member ID
- Name and address (city, state or province, and country) of the Merchant declared to be fully collusive
- MasterCard *Global Security Bulletin* (number and date) that listed the fully collusive Merchant
- Total number of Transactions processed at the fully collusive Merchant
- Total dollar volume of Issuer losses at the fully collusive Merchant, as reported to SAFE
- Percent of collusive Transactions attributed to Cardholder bust-out accounts
- Credit limit in effect at the time the Cardholder bust-out account was closed
- Amount of losses incurred subsequent to exhaustion of Cardholder bust-out account credit limit
- Date of initial Issuer notification to MasterCard (as provided in the relevant *Global Security Bulletin*)
- Amount of losses incurred subsequent to the date of initial Issuer notification to MasterCard
- Date that MasterCard notified the Issuer of the suspected fully collusive Merchant to validate account status
- Amount of losses incurred subsequent to MasterCard notification to the Issuer to validate account status

Attach documentation containing the following information:

- Complete details of Issuer-confirmed collusive Transactions, including account number, Transaction date and time, and Transaction amount in U.S. dollars
- Amount of fraud reported to SAFE with fraud type code 51 (Bust-out Collusive Merchant) and the reported date
- A report of the Issuer's investigative findings concerning the fully collusive Merchant
- Complete details of the Issuer's contacts with the Acquirer concerning the fully collusive Merchant, specifying dates and subject matter
- Complete details of the Issuer's knowledge of law enforcement involvement
- Complete details of the Issuer's tracking system (procedures for NSF checks, credit report monitoring, and similar measures)

8.4.8.2 Required Acknowledgement

Issuers must acknowledge and certify that the Cardholder bust-out account Transactions submitted have been reported to MasterCard, entered into SAFE under fraud type code 51 (Bust-out Collusive Merchant), and adhere to the Cardholder bust-out account definition. In addition, Issuers must certify, for the Transactions and Cardholder accounts included in the claim filing, that:

- Each Transaction occurred before the publication date of the *Global Security Bulletin* declaring the Merchant as fully collusive.
- No other recovery was received, via any existing remedy in the MasterCard system, recovery process, or the Issuer's own collection process, for any of the Transactions.
- No first party fraud (fraudulent application or account takeover) Transactions were included in the claim.
- Appropriate screening of the Cardholder(s) involved was conducted at the time of Card issuance and in compliance with the financial institution, industry, and regulatory acquisition policies and best practices, including but not limited to a review of the Cardholder's credit report and continued monitoring of the Cardholder's account.

The Issuer's Principal Contact must sign and date this acknowledgement and certification.

Chapter 9 MasterCard Registration Program

This chapter may be of particular interest to Customer personnel responsible for registering Merchants 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.....	9-1
9.2 General Registration Requirements.....	9-1
9.2.1 Merchant Registration Fees and Noncompliance Assessments.....	9-3
9.2.2 Service Provider Registration Noncompliance Assessments.....	9-3
9.3 General Monitoring Requirements.....	9-4
9.4 Additional Requirements for Specific Merchant Categories.....	9-4
9.4.1 Key-entry Telecom Merchants.....	9-4
9.4.2 Other Telecom Merchants and Transactions.....	9-5
9.4.3 Electronic Commerce Adult Content (Videotext) Merchants.....	9-6
9.4.4 Non-face-to-face Gambling Merchants.....	9-6
9.4.5 Prescription Drug and Tobacco Merchants.....	9-8
9.4.6 State Lottery Merchants (U.S. Region Only).....	9-9

9.1 MasterCard Registration Program Overview

MasterCard requires Customers to register the following Merchant types and other entities using the MasterCard Registration Program (MRP) system, available via MasterCard OnLine®:

- Telecom Merchants—MCCs 4813, 4814, 4816, and 5967 (refer to [section 9.4.1](#) and [section 9.4.2](#))
- Electronic commerce (e-commerce) adult content (videotext) Merchants—MCCs 5967, 7273, and 7841 (refer to [section 9.4.3](#))
- Non-face-to-face gambling Merchants—MCCs 7995 and 9754 (refer to [section 9.4.4](#))
- Non-face-to-face prescription drug Merchants—MCC 5122 and MCC 5912 (refer to [section 9.4.5](#))
- Non-face-to-face tobacco product Merchants—MCC 5993 (refer to [section 9.4.5](#))
- State lottery Merchants (U.S. region only)—MCC 9399 (refer to [section 9.4.6](#))
- Merchants reported under the Excessive Chargeback Program (refer to [section 8.3](#))
- Any Third Party Processor (TPP), Independent Sales Organization (ISO), Data Storage Entity (DSE), or other person that performs or proposes to perform Program Services for the Customer or in connection with the Customer's Program. Service Providers may be registered either using the MRP system or through a Service Provider Registration Facilitator.

If a Customer acquires Transactions for any of the Merchant types listed herein without first registering the Merchant 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.

Refer to the *MATCH User Manual* for technical information about the use of the MRP system.

9.2 General Registration Requirements

The Customer must provide all of the information requested for each Merchant, ISO, TPP, DSE, or other entity required to be registered through the MasterCard Registration Program system. For each such entity, the requested information includes:

MasterCard Registration Program

9.2 General Registration Requirements

- The name, doing business as (DBA) name, and address
- The central access phone number, customer service phone number, or e-mail 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, Merchants, or Service Providers
- A description of payment processing procedures, Cardholder or Merchant 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

An entity proposed for registration as a TPP or DSE must comply with the MasterCard Site Data Protection (SDP) Program in accordance with the implementation schedule set forth in [section 10.3.4](#) of this manual. Before initiating registration, the Customer must instruct the proposed TPP or DSE to contact MasterCard via e-mail at sdp@mastercard.com and to validate its compliance with the MasterCard SDP Program using the tools described in [section 10.3.2](#), or if the proposed TPP is not compliant, to provide a compliance plan approved by MasterCard. For Service Provider registration requirements, refer to MasterCard Rule 7.6.

All of the information required to complete the registration of a Service Provider must be provided **within 60 days** of the registration application submission date. For a proposed TPP or DSE, such information includes but is not limited to validation of compliance with the MasterCard SDP Program.

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 explanation for the request. MasterCard reserves the right to deny a modification request.

Customers should send any additional requested information and modification requests to the vice president of Merchant Fraud Control at the address provided in [Appendix C](#).

For requirements specific to Merchants, TPPs, and DSEs that are required to implement the MasterCard 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 1,000 registration fee for each Merchant under the categories listed in [section 9.1](#), except telecom Merchants and Merchants reported under the Excessive Chargeback Program. MasterCard will collect the fee from the Acquirer via the MasterCard Consolidated Billing System (MCBS).

MasterCard may assess a Customer that acquires Transactions for any of these Merchant types without first registering the Merchant in accordance with the requirements of the MRP. A violation will result in an assessment of up to USD 5,000.

If, after notice by MasterCard of the Acquirer's failure to register a Merchant, that Acquirer fails to register its Merchant within 10 days of notice, the Acquirer will be subject to additional assessments of up to USD 25,000 until the Acquirer satisfies the requirement. In addition, the Acquirer must ensure that the violation is corrected promptly.

If any such Merchant exceeds USD 25,000 in fraud in any calendar month, the Acquirer will be subject to the assessments shown in Table 9.1.

Table 9.1–Noncompliance Assessments

Months of Noncompliance ¹	Assessment
1	USD 25,000
2	USD 100,000
3	USD 150,000

9.2.2 Service Provider Registration Noncompliance Assessments

MasterCard may assess a Customer that directly or indirectly receives Program Services from any person that the Customer has not registered as a Service Provider as described in MasterCard Rule 7.6.3.

1. Months may be non-consecutive.

9.3 General Monitoring Requirements

The monitoring requirements described in this section apply to Customers that acquire telecom Transactions, e-commerce adult content (videotext) Transactions, non-face-to-face gambling Transactions, non-face-to-face prescription drug and tobacco product Transactions, state lottery Transactions (U.S. region only), or Transactions from Merchants reported under the Excessive Chargeback Program:

- 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 Card account number
 - Consecutive or excessive attempts using the same Card account numberWhen 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 Excessive Chargeback Program thresholds. For information about the Excessive Chargeback Program, refer to [section 8.3](#) of this manual.
- On a quarterly basis, the Acquirer must submit monthly Transaction data to MasterCard (via the MRP) for the Acquirer's registered Merchants. This data contains sales (counts and amounts), chargebacks (counts and amounts), and credits (counts and amounts) by calendar month. If preferred, the Acquirer may submit this data on a monthly basis.

9.4 Additional Requirements for Specific Merchant Categories

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

9.4.1 Key-entry Telecom Merchants

A key-entered telecom Transaction occurs when a person calls a central access phone number to access a system that enables the placement of a subsequent local or long-distance call, and bills the cost of the call(s) to a Cardholder's Card account. The account number and expiration date are entered using the phone key pad. The Transactions may include, but are not limited to, voice calls, fax calls, data connections, or other dialed connections using voice or data lines.

A key-entry telecom Merchant enters a Merchant Agreement with an Acquirer to initiate key-entered telecom Transactions, which must be identified with Card acceptor business code (MCC) 4813 and Transaction Category Code (TCC) T. These codes specify a key-entry telecom Merchant providing single local and long-distance phone calls using a central access number in a non-face-to-face environment using key entry.

Before an Acquirer may process key-entered telecom Transactions from a Merchant, it must register the Merchant with MasterCard as described in [section 9.2](#).

The Acquirer must maintain an individual fraud control action plan for each of its key-entered telecom Merchants before acquiring these Transactions. MasterCard may request a copy of this action plan and require changes as a condition to the initiation or continuation of acquiring key-entered telecom Transactions.

The Acquirer continuously must monitor:

- Call duration
- Originating and terminating phone number frequency
- Multiple geographic origins for the same account
- High-risk countries
- Known fraud-prone account numbers
- Originating and terminating phone numbers known to be used for fraud or attempted fraud

9.4.2 Other Telecom Merchants and Transactions

Telecom Transactions, such as prepaid phone services, recurring phone services, Card-read Transactions, and Transactions originating from audiotext Merchants and Internet service providers differ from key-entered telecom Transactions, and should be reported using the appropriate MCC and TCC combinations:

- **MCC 4814, TCC T—Telecommunication Services, including, but not limited to, prepaid phone services and recurring phone services.** This type of Transaction includes the use of a Card in both Card-reading and non-Card-reading environments. It may include prepaid and recurring phone service Transactions or other telecommunications services.
- **MCC 4816, TCC T—Computer Network/Information Services.** This MCC identifies providers of computer network, information services, and other online services such as e-mail or Internet access.
- **MCC 5967, TCC T—Direct Marketing—Inbound Telemarketing Merchants.** This MCC includes providers of information services offered over the phone (audiotext) or Internet (videotext). An audiotext call is a pay-per-call service whereby a Merchant provides audio information or entertainment to a Cardholder by phone. The Cardholder is charged either per call or per time interval, in addition to or at a rate more than the charge paid for the transmission of the call.

9.4.3 Electronic Commerce Adult Content (Videotext) Merchants

An electronic commerce adult content (videotext) Transaction occurs in a Card-not-present environment when a consumer uses a MasterCard account to purchase videotext adult services.

Acquirers must identify all electronic commerce adult content (videotext) Transactions using MCC 5967 (Direct Marketing—Inbound Telemarketing Merchants) and TCC T. For Merchants that provide dating and escort services, including computer and video personal introduction and matchmaking services, Acquirers must use MCC 7273 (Dating and Escort Services). For Merchants that rent adult content videotapes and DVDs, Acquirers must use MCC 7841 (Video Entertainment Rental Stores).

Before an Acquirer may process electronic commerce adult content (videotext) Transactions from a Merchant, it must register the Merchant with MasterCard as described in [section 9.2](#) of this manual.

9.4.4 Non-face-to-face Gambling Merchants

A non-face-to-face gambling Transaction occurs in a Card-not-present environment when a consumer uses a Card 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 7995 (Gambling Transactions) or MCC 9754 (Gambling—Horse Racing, Dog Racing).

Before acquiring Transactions reflecting non-face-to-face gambling, an Acquirer first must register the Merchant with MasterCard as described in [section 9.2](#). Acquirers must identify all non-face-to-face gambling Transactions using MCC 7995 and TCC U unless the Acquirer has also registered the Merchant as described below, in which case the Acquirer may use MCC 9754 instead of MCC 7995.

In addition to the requirement to register the Merchant as described in section 9.2, a U.S. region Acquirer may register a Merchant under this section if the Merchant is located in the U.S. region and engaged in gambling activity involving horse racing or dog racing. To register such a Merchant, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items to MasterCard as part of the registration process:

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 private sector U.S. lawyer or U.S. law firm. 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, 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 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 MasterCard Rule 3.3 regardless of the Acquirer's compliance with the MasterCard *Internet Gambling Policy* or these requirements.

All non-face-to-face gambling Transactions must include the indent-printed CVC 2 value in Data Element (DE) 48 (Additional Data—Private Use), subelement 92 (CVC 2) of the Authorization Request/0100 message.

Acquirers must process non-face-to-face gambling Transactions in accordance with MasterCard Rule 5.1.2.2.

9.4.5 Prescription Drug and Tobacco Merchants

A non-face-to-face prescription drug Transaction occurs in a Card-not-present environment when a consumer uses a Card 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 a Card account to purchase tobacco products (including, but not limited to cigarettes, cigars, or loose tobacco) from a Merchant whose primary business is non-face-to-face selling of tobacco products.

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

- Non-face-to-face sale of prescription drugs (MCC 5122 and MCC 5912)
- Non-face-to-face sale of tobacco products (MCC 5993)

Acquirers must identify all non-face-to-face prescription drug 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. Acquirers 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 MasterCard Rule 3.3.

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

By registering a Merchant 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 that is subject to the aforescribed registration requirement and must, no less frequently than every 12 months, confirm continued compliance with applicable law concerning the business of the registered Merchant. The Acquirer must furnish MasterCard with a copy of such documentation promptly upon request.

9.4.6 State Lottery Merchants (U.S. Region Only)

A U.S. region Acquirer may use MCC 9399 (Government Services—not elsewhere classified) to identify Transactions arising from a U.S. region Merchant and involving the purchase of a state lottery ticket if the Acquirer has first registered the Merchant with MasterCard as described in section 9.2 and this section 9.4.6.

To register such a Merchant, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items to MasterCard as part of the registration process:

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:

MasterCard Registration Program

9.4 Additional Requirements for Specific Merchant Categories

- 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 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 MasterCard Rule 3.3 regardless of the Acquirer's compliance with MasterCard rules, policies, and procedures or these requirements.

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	10-1
10.2 Account Data Compromise Events	10-1
10.2.1 Policy Concerning Account Data Compromise Events and Potential Account Data Compromise Events	10-2
10.2.2 Responsibilities in Connection with ADC Events and Potential ADC Events.....	10-3
10.2.2.1 Time-Specific Procedures for ADC Events and Potential ADC Events	10-3
10.2.2.2 Ongoing Procedures for ADC Events and Potential ADC Events	10-5
10.2.3 Forensic Report	10-6
10.2.4 MasterCard Determination of ADC Event or Potential ADC Event	10-8
10.2.4.1 Assessments for PCI Violations in Connection with ADC Events	10-8
10.2.4.2 Potential Reduction of Financial Responsibility	10-8
10.2.4.3 ADC Operational Reimbursement and ADC Fraud Recovery	10-10
10.2.4.4 ADC Operational Reimbursement Calculation.....	10-10
10.2.4.5 ADC Fraud Recovery	10-11
10.2.4.6 Investigation and Other Costs	10-11
10.2.5 Assessments for Noncompliance	10-11
10.3 MasterCard Site Data Protection (SDP) Program	10-12
10.3.1 Payment Card Industry Data Security Standards.....	10-12
10.3.2 Compliance Validation Tools.....	10-13
10.3.3 Acquirer Compliance Requirements	10-13
10.3.4 Implementation Schedule.....	10-15
10.3.4.1 MasterCard PCI DSS Risk-based Approach.....	10-19
10.3.4.2 Mandatory Compliance Requirements for Compromised Entities.....	10-20
10.4 Connecting to MasterCard—Physical and Logical Security Requirements	10-21
10.4.1 Minimum Security Requirements	10-21
10.4.2 Additional Recommended Security Requirements	10-22
10.4.3 Ownership of Service Delivery Point Equipment.....	10-22

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 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 Transmission Security Program (PCI PTS) and *Payment Card Industry Data Security Standard* (PCI DSS). Customers and their agents also must ensure that:

- a terminal or other device at the Point of Interaction (POI) does not display, replicate, or store any Card-read data except Card account number, expiration date, service code, or Cardholder name; and
- before discarding any media containing Card, Cardholder, or Transaction data, including such data as account numbers, personal identification numbers (PINs), credit limits, and account balances, the Customer or its agent must render the data unreadable; and
- access to Card, Cardholder, or Transaction data stored in computers, terminals, and PCs is limited and controlled by establishing data protection procedures that include, but are not limited to, a password system for Computer Remote Terminal (CRT) access, control over dial-up lines, and any other means of access.

10.2 Account Data Compromise Events

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 MasterCard account data.

Agent

Any entity that stores, processes, or has access to MasterCard 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](#) section at the front of the manual. For the avoidance of doubt, for purposes of this section 10.2, any entity that MasterCard licenses to issue a Card(s) and/or acquire a Transaction(s) shall be deemed a Customer.

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 MasterCard account data.

Standards

This term appears in the [Definitions](#) section at the front of the manual.

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.

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 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).

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 becomes aware 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.

Account Data Protection Standards and Programs

10.2 Account Data Compromise Events

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 MasterCard 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 account numbers and expiration dates associated with MasterCard 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 account numbers to MasterCard applies to any MasterCard or Maestro account number in a bank identification number (BIN) range assigned by MasterCard. This obligation applies regardless of how or why such account numbers 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 qualified incident response assessor (“QIRA”) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration and effects of the ADC Event or Potential ADC Event. The QIRA 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 QIRA’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.

- Within two (2) business days from the date on which the QIRA was engaged, identify to MasterCard the engaged QIRA and confirm that such QIRA has commenced its investigation.
- Within three (3) business days from the commencement of the forensic investigation, ensure that the QIRA 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 QIRA, 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 any (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 QIRA 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 QIRA 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 QIRA to withhold information from MasterCard.

Notwithstanding the foregoing, MasterCard may engage a QIRA on behalf of the Customer in order to expedite the investigation. The Customer on whose behalf the QIRA 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:

Account Data Protection Standards and Programs

10.2 Account Data Compromise Events

- 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 QIRA 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 QIRA 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 QIRA 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 QIRA retain and safeguard all draft forensic report(s) pertaining to the ADC Event or Potential ADC Event and, upon request of MasterCard, immediately provide 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 QIRA.
- 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 Point-of-Sale (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 MasterCard 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 MasterCard 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 MasterCard 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 MasterCard account data at risk of compromise, including the number of MasterCard accounts and at risk data elements (magnetic stripe data—Track 1 and Track 2, Cardholder name, primary account number [PAN], expiration date, Card validation code [CVC] 2, PIN, and PIN block).
- The location and number of MasterCard accounts where restricted account data (magnetic stripe, Track 1 and Track 2, Cardholder name, PAN, expiration date, CVC 2, PIN, or PIN block), whether encrypted or unencrypted, was or may have been stored by the entity that was the subject of the forensic investigation. This includes restricted MasterCard 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 MasterCard accounts determined to be at risk of compromise. If Transaction date/time is not able to be determined, file-creation timestamps must be supplied.
- A determination of whether a security breach that exposed payment card data to compromise occurred.
- On a requirement-by-requirement basis, a conclusion as to whether, at the time the ADC Event or Potential ADC Event occurred, each applicable PCI Security Standards Council 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 QIRA to conduct a PCI GAP analysis and include the result of that analysis in the final forensic report.

The Customer must direct the QIRA to submit a copy of the preliminary and final forensic reports to MasterCard via Secure Upload.

10.2.4 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 QIRA report; or
- any information determined by MasterCard to be sufficiently reliable at the time of receipt.

10.2.4.1 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 Security Standards Council.

10.2.4.2 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 MasterCard 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. Effective 1 July 2012, 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 PCI SSC Forensic Investigator (PFI) has validated that the Merchant was compliant with milestones one through four 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 under the MasterCard Registration Program (MRP), in accordance with Chapter 9 of this manual.
- 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 Merchant Acquirer Contact as they are listed in the Member Information tool, 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 tool.

10.2.4.3 ADC Operational Reimbursement and ADC Fraud Recovery

ADC operational reimbursement enables an Issuer to partially recover costs incurred in reissuing Cards and for enhanced monitoring of compromised and/or potentially compromised accounts associated with an ADC Event. ADC fraud recovery enables an Issuer to recover partial incremental magnetic-stripe (POS 90) and/or chip Card terminal unable to process (POS 80) counterfeit fraud losses associated with an ADC Event. MasterCard determines ADC operational reimbursement and ADC fraud recovery.

ADC operational reimbursement and ADC fraud recovery are available to an Issuer that is licensed to access MasterCard Alerts at the time of the ADC Event. MasterCard reserves the right to determine which ADC Events will be eligible for ADC operational reimbursement and/or ADC fraud recovery and to limit or “claw back” ADC operational reimbursement and ADC fraud recovery based on the amount collected from the responsible Customer, excluding assessments.

MasterCard will charge the Issuer an administrative fee as established from time to time for administering the ADC operational reimbursement and ADC fraud recovery processes.

Under the ADC operational reimbursement and ADC fraud recovery programs, MasterCard calculates the total Customer liability for each ADC Event. MasterCard may limit compensation to affected Customers taking into consideration the compromised entity’s PCI level (as set forth in [section 10.3.4](#)), annual sales volume and, to the extent possible, the factors set forth in [section 10.2.4.2](#).

The annual sales volume is derived from the Merchant’s clearing Transactions processed during the previous year via 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.

10.2.4.4 ADC Operational Reimbursement Calculation

Subject to [section 10.2.4.3](#), MasterCard will calculate ADC operational reimbursement using the following method:

1. Determine the total number of accounts per ICA number that were at risk by type of Card, utilizing an assumption of one Card per account.
2. Subtract a fixed deductible (which will be updated and published yearly in the *Global Security Bulletin*), to account for normal Card expirations, Card re-issuance cycles, accounts included in previous MasterCard Alerts and re-issuance of accounts using the same PAN but a different expiration date.
3. Multiply the number of accounts by an amount set by MasterCard from time to time.

10.2.4.5 ADC Fraud Recovery

Subject to section 10.2.4.3, MasterCard will calculate the amount of incremental counterfeit fraud attributable to an ADC Event based on the fraud data reported to the System to Avoid Fraud Effectively (SAFE).

If a Customer changes the fraud type reported to SAFE after MasterCard calculates the ADC fraud recovery amount, MasterCard will not recalculate the ADC fraud recovery amount.

ADC fraud recovery calculation uses an “at-risk time frame.” The at-risk time frame may be known or not known.

The at-risk time frame is known when MasterCard is able to determine the period of time during which accounts were at risk due to or in connection with an ADC Event. In such event, the at-risk time frame for a particular account number (i) is deemed to commence as of the date that MasterCard determines that account was at risk, and (ii) is deemed to end 30, 45, or 60 days after the date of publication of the earliest MasterCard Alert that discloses the account number (as more particularly described in the *ADC User's Guide*).

If the at-risk time frame is not known, the at-risk time frame for a particular account number (i) is deemed to commence twelve (12) months prior to the date of publication of the earliest MasterCard Alert that discloses that account number, and (ii) is deemed to end 30, 45, or 60 days after the date of publication of the earliest MasterCard Alert that discloses the account number (as more particularly described in the *ADC User's Guide*).

The ADC fraud recovery calculation further provides that an account number published in a MasterCard Alert in connection with a different ADC Event during the six (6) months prior to the publication of the MasterCard Alert published in connection with the subject ADC Event is removed from the list of account numbers eligible for ADC fraud recovery. In addition, a standard deductible (to be updated annually) will be applied to recognize chargeback recoveries on Transactions using at-risk accounts and prior reissuance of at-risk account numbers with different expiration dates.

10.2.4.6 Investigation and Other Costs

MasterCard may assess the responsible Customer for all investigation and other costs incurred by MasterCard in connection with an ADC Event and may assess a Customer for all investigative and other costs incurred by MasterCard in connection with a Potential ADC Event.

10.2.5 Assessments 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 per day for each day the Customer is noncompliant.

10.3 MasterCard Site Data Protection (SDP) Program

The MasterCard Site Data Protection (SDP) Program is designed to encourage Customers, Merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect against account data compromises. SDP facilitates the identification and correction of vulnerabilities in security processes, procedures, and Web site configurations. For the purposes of the SDP Program, TPPs and DSEs are collectively referred to as “Service Providers” in this chapter.

Acquirers must implement the MasterCard SDP Program by ensuring that their 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 their 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 SDP; 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 account data compromise.

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

10.3.1 Payment Card Industry Data Security Standards

The *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* establish data security requirements. Compliance with the *Payment Card Industry Data Security Standard* is required for all Issuers, Acquirers, Merchants, Service Providers, and any other person or entity a Customer permits, directly or indirectly, to store, transmit, or process account data. MasterCard requires validation of compliance only for those entities specified in the SDP Program implementation schedule in [section 10.3.4](#). Effective 1 July 2012, 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. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*.

The *Payment Card Industry Data Security Standard*, the *Payment Card Industry Payment Application Data Security Standard*, the *PCI PA-DSS Program Guide*, and other PCI Security Standards manuals are available on the PCI Security Standards Council Web site at www.pcisecuritystandards.org.

10.3.2 Compliance Validation Tools

As defined 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* by using the following tools:

- **Onsite Reviews**—The onsite review evaluates Merchant or Service Provider compliance with the *Payment Card Industry Data 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 Web site. Onsite reviews must be conducted in accordance with the *Payment Card Industry Security Audit Procedures* manual.
- **The Payment Card Industry Self-assessment Questionnaire**—The *Payment Card Industry Self-assessment Questionnaire* is available at no charge on the PCI Security Standards Council Web site. 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 Web site. 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 Web site. To be compliant, scanning must be conducted in accordance with the guidelines contained in the *Payment Card Industry DSS Security Scanning Procedures* manual.

10.3.3 Acquirer Compliance Requirements

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

Account Data Protection Standards and Programs

10.3 MasterCard Site Data Protection (SDP) Program

- For each Level 1, Level 2, and Level 3 Merchant, submit a quarterly status report via an e-mail message to sdp@mastercard.com using the form provided on the SDP Program Web site. 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.

In submitting a quarterly 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 TPP or DSE 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 via a Web page and therefore store account data temporarily in memory files. Per 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 and DSEs.

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.

Effective 1 July 2012, 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 Security Standards Council Web site at www.pcisecuritystandards.org as 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*.

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*:

Account Data Protection Standards and Programs

10.3 MasterCard Site Data Protection (SDP) Program

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

Effective 30 June 2012, 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 PCI SSC associated 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.

Effective 30 June 2012, 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 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 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, though validation of compliance (and all other MasterCard SDP Program Acquirer requirements set forth in [section 10.3.3](#)) 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 account data compromise 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.

If a Level 4 Merchant has validated its compliance with the *Payment Card Industry Data Security Standard* and effective 1 July 2012, 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 (regardless of volume) and any DSE 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* by successfully completing:

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

Level 2 Service Providers

A Level 2 Service Provider is any DSE 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.

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.

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
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 or DSE as a Service Provider, or termination of the Acquirer as a Customer as provided in MasterCard Rule 1.6.2.

The Acquirer must provide compliance action plans and quarterly compliance status reports for each Level 1, Level 2, and Level 3 Merchant using the SDP Acquirer Submission and Compliance Status Form, available at <http://www.mastercard.com/us/sdp/index.html> 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) via e-mail message to sdp@mastercard.com on or before the last day of the quarter, as indicated below.

For this quarter...	Submit the form(s) no later than...
1 January to 31 March	31 March
1 April to 30 June	30 June
1 July to 30 September	30 September
1 October to 31 December	31 December

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 MasterCard Rule 3.1.2.

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, under which the Merchant:

- Validates compliance with the first four of the six total milestones set forth in the *PCI DSS Prioritized Approach*, as follows:
 - Level 1 Merchants 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.
 - Level 2 Merchants 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 via an onsite assessment.
- Annually revalidates compliance with milestones one through four using an SAQ. The SAQ must be completed by internal staff trained and currently certified through the PCI SSC-offered ISA Program.

To qualify, the Merchant must meet all of the following criteria:

Account Data Protection Standards and Programs

10.3 MasterCard Site Data Protection (SDP) Program

- The Merchant must certify that it is not storing sensitive Card authentication data.
- The Merchant must fully segregate its Card-not-present Transaction environment from its face-to-face Transaction environment. A face-to-face Transaction occurs when the Card, the Cardholder, and the Merchant representative are all present at the time 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 South Asia/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 been involved in 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 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 TPP or DSE, or by its Acquirer, if the compromised entity is a Merchant. The form must be returned via e-mail to pci-adc@mastercard.com within 30 calendar days of its receipt, and must include:

- The names of the Qualified Security Assessor (QSA) and the Approved Scanning Vendor (ASV) that conducted the forensics evaluation, and
- The entity's current level of compliance with the *Payment Card Industry Data Security Standard*, and
- A gap analysis providing detailed steps required for the entity to achieve full compliance with the *Payment Card Industry Data Security Standard*.

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*.

Such evidence (for example, a letter attesting to the entity's compliance, a compliance certificate, or a compliance status report) must be submitted to MasterCard via e-mail 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 Level 1 or Level 2 Service Provider that has suffered a confirmed account data compromise 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 Worldwide 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).

Account Data Protection Standards and Programs

10.4 Connecting to MasterCard—Physical and Logical Security Requirements

4. The Customer or its agent must conduct regular periodic reviews of all systems and devices that store MasterCard 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 C](#) 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 Worldwide 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

MasterCard is the sole and exclusive owner of all Service Delivery Point Equipment placed by MasterCard at the Service Delivery Point.

Effective as of date of placement, the Customer is granted a nonexclusive, non-assignable License to use the Service Delivery Point Equipment. The Customer may not take any action adverse to MasterCard with respect to its ownership 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 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 Member Alert to Control High-risk (Merchants) (MATCH™) system.

- 11.1 MATCH Overview 11-1
 - 11.1.1 System Features 11-1
 - 11.1.2 How does MATCH Search when Conducting an Inquiry? 11-2
 - 11.1.2.1 Retroactive Possible Matches 11-2
 - 11.1.2.2 Exact Possible Matches 11-3
 - 11.1.2.3 Phonetic Possible Matches 11-4
- 11.2 MATCH Standards 11-4
 - 11.2.1 Certification 11-5
 - 11.2.2 When to Add a Merchant to MATCH 11-5
 - 11.2.3 Inquiring about a Merchant 11-6
 - 11.2.6 MATCH Record Retention 11-6
- 11.4 Merchant Removal from MATCH 11-6
- 11.5 MATCH Reason Codes 11-7
 - 11.5.1 Reason Codes for Merchants Listed by the Acquirer 11-7

11.1 MATCH Overview

MasterCard designed MATCH™, the Member Alert to Control High-risk (Merchants) system, 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 Acquirers. 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.

WARNING!

MasterCard does not verify, otherwise confirm, or ask for confirmation of either the basis for or accuracy of any information that is reported to or listed in MATCH. It is possible that information has been wrongfully reported or inaccurately reported. It is also possible that facts and circumstances giving rise to a MATCH report may be subject to interpretation and dispute.

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 per 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 the system returns.
- MATCH processes data submitted by Acquirers once per day and provides daily detail response files.
- Acquirers may access MATCH data online in real time using a PC at the Acquirer's site.

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
Business Name			= ✓
Business Phone Number			= ✓
Business National Tax ID	+ Country		= ✓
Business State Tax ID	+ State		= ✓
Business Street Address	+ City	+ State ¹	= ✓
Business Street Address	+ City	+ Country ²	= ✓
Principal Owner's (PO) First Initial	+ Last Name		= ✓
PO First Name	+ Last Name		= ✓
PO Phone			= ✓
PO Social Security Number ¹			= ✓
PO National ID ²			= ✓
PO Street Address (lines 1 and 2)	+ PO City	+ PO State ¹	= ✓
PO Street Address (lines 1 and 2)	+ PO City	+ PO Country ²	= ✓
PO Driver's License (DL) Number	+ DL State ¹		= ✓
PO Driver's License Number	+ DL Country ²		= ✓

NOTE

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

1. If country is USA.

2. If country is not USA.

MATCH System

11.2 MATCH Standards

11.1.2.3 Phonetic Possible Matches

The MATCH system converts certain alphabetic data, such as Business 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
Business Name					=	√
Doing Business As (DBA) Name					=	√
Business Street Address	+	City	+	State ³	=	√
Business Street Address	+	City	+	Country ⁴	=	√
Principal Owner’s (PO) First Initial	+	Last Name			=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO State ³	=	√
PO Street Address (lines 1 and 2)	+	PO City	+	PO Country ⁴	=	√

NOTE

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

11.2 MATCH Standards

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

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

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

3. If country is USA

4. If country is not USA

5. Acquirers globally are assessed an annual MATCH usage fee of USD 4,000. In addition, Acquirers are assessed a MATCH inquiry fee (per Member ID/ICA number) for each MATCH inquiry.

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, and 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 for reporting compliance reasons. If an Acquirer does not conduct the inquiry under the proper Member ID (that is, the Member ID 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 Merchant Fraud Control. 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

Refer to [section C.2](#) of Appendix C of this manual for the contact information of Merchant Fraud Control.

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.

MATCH System

11.5 MATCH Reason Codes

Table 11.3–MATCH Listing Reason Codes Used by Acquirers

MATCH Reason Code	Description
01	Account Data Compromise The Merchant unknowingly or unintentionally facilitated, by any means, the unauthorized disclosure or use of account information.
02	Common Point of Purchase (CPP) The Merchant knowingly caused or facilitated, by any means, the unauthorized disclosure or use of account information.
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 Merchant's chargebacks in any single month exceeded 1% of its 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 (Refer to Table 11.5)
07	Fraud Conviction There was a criminal fraud conviction of a principal owner or partner of the Merchant.
08	Reserved for Future Use (Refer to Table 11.5)
09	Bankruptcy/Liquidation/Insolvency The Merchant was unable or is likely to become unable to discharge its financial obligations.

MATCH Reason Code	Description
10	<p>Violation of Standards</p> <p>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 <i>MasterCard Rules</i> manual.</p> <p>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.</p>
11	<p>Merchant Collusion</p> <p>The Merchant participated in fraudulent collusive activity.</p>
12	<p>PCI Data Security Standard Noncompliance</p> <p>The Merchant failed to comply with <i>Payment Card Industry (PCI) Data Security Standard</i> requirements.</p>
13	<p>Illegal Transactions</p> <p>The Merchant was engaged in illegal Transactions.</p>
14	<p>Identity Theft</p> <p>The Acquirer has determined 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.</p>

Two additional reason codes may apply to Merchants listed in MATCH. Acquirers no longer may add Merchants to MATCH using the reason codes in Table 11.5; however, these codes still may appear in legacy MATCH reports.

Table 11.4–MATCH Reason Codes No Longer Available for Listing Purposes

MATCH Reason Code	Description
06	<p>Violation of Merchant Agreement</p> <p>The Merchant was in violation of a significant term or condition of the Merchant Agreement. As used herein, a significant term or condition means one that concerns the truthfulness of the Merchant or the commercial reasonableness of the Merchant's manner of doing business and does not mean a technical violation of the Merchant Agreement, such as one resulting in a minor financial dispute.</p>
08	<p>MasterCard Audit Program Thresholds</p> <p>The Merchant exceeded thresholds for counterfeit or other fraud or chargeback activity or the like established periodically by MasterCard.</p>

Chapter 12 Omitted

This chapter has been omitted.

Chapter 13 Fraud Management Program (FMP)

This chapter describes the Fraud Management Program (FMP) Standards and applies to all Issuers, Acquirers, and Service Providers.

13.1 About FMP 13-1
 13.1.2 FMP Level 2 Service Provider Reviews 13-1

13.1 About FMP

The MasterCard Fraud Management Program (FMP) is a tool for assessing a Customer's current capability to manage, anticipate, and protect against inherent internal and external risks in the issuing and acquiring portfolio.

FMP also determines the effectiveness of existing fraud loss controls and other risk reduction measures and assists Customers in identifying specific areas where such measures may be inadequate.

In addition, FMP provides, where appropriate, 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.

FMP consists of three mandatory levels and one optional level. The three mandatory levels are Level 1 reviews for prospective Principals and Affiliates, Level 2 Service Provider reviews, and Level 3 Customer reviews. Customers may also choose to participate in Level 4 Customer Consultative reviews. This chapter describes the Standards for each review level.

13.1.2 FMP Level 2 Service Provider Reviews

The FMP Level 2 Service Provider review is an annual review conducted for selected Service Providers, at the sole discretion of Security and Risk Services staff.

MasterCard will examine the Service Provider's ability to support Customers so that they can adhere to the minimum fraud loss control Program requirements described in [Chapter 6](#) of this manual.

A Service Provider that fails an FMP Level 2 Service Provider review is subject to deregistration.

Chapter 14 Omitted

This chapter has been omitted.

Chapter 15 Omitted

This chapter has been omitted.

Appendix A Omitted

This chapter has been omitted.

Appendix B Formset Specifications

This appendix contains specifications for the interchange copy of MasterCard® Card Transaction formsets.

B.1 MasterCard Formset Specifications	B-1
B.1.1 Formset Physical Dimensions	B-1
B.1.2 Number of Copies and Retention Requirements.....	B-1
B.1.3 Paper Stock Characteristics	B-1
B.1.4 Color of Interchange Copy	B-1
B.1.5 Carbon.....	B-1
B.1.6 Registration Mark	B-2
B.1.6.1 Registration Mark Location.....	B-2
B.1.7 Formset Numbering.....	B-2
B.1.7.1 Formset Number Location.....	B-2
B.1.8 Information Slip Specifications	B-3
B.2 Formset Printing Standards	B-3
B.2.1 Retail Sale, Credit, and Cash Disbursement Formsets.....	B-3
B.2.2 Information Slip Formsets.....	B-4
B.2.3 Imprinters	B-4

B.1 MasterCard Formset Specifications

A formset is a Transaction information document (TID) produced with a manual imprinter. This appendix describes the Standards for the interchange copy of retail sale, credit, cash disbursement, and information formsets for Transactions, including physical dimensions, weight, color, carbon paper, registration marks, numbering, and printing.

B.1.1 Formset Physical Dimensions

Formsets must be the size of a standard 80-column Card (3.250 inches x 7.375 inches, or 8.260 cm x 18.744 cm) or a standard 51-column Card (3.250 inches x 4.852 inches, or 8.260 cm x 12.332 cm), with an upper right-hand corner cut.

B.1.2 Number of Copies and Retention Requirements

Each formset must consist of at least two copies, one complete copy for the Merchant/Acquirer, and one complete copy for the customer. MasterCard recommends that the Merchant or the Acquirer process the copy signed by the Cardholder. If this is the only copy retained, the Merchant must hold the copy (microfilm or otherwise reproduced copy) for at least 18 months to satisfy the MasterCard retention requirement.

B.1.3 Paper Stock Characteristics

Formsets must be no less than 28-pound stock and no more than 103-pound stock, U.S. region Standards.

B.1.4 Color of Interchange Copy

The color of the interchange copy of a formset must be manila or white if Card stock (for example, 95-pound stock, U.S. region standards or heavier), and must be white if paper stock (for example, 28-pound stock, U.S. region standards or heavier but less than 95-pound stock).

B.1.5 Carbon

The carbon paper used to imprint the interchange copy of a formset must be black and of optical character recognition (OCR) quality. All formsets ordered by Customers supplying formsets to Merchants must be manufactured so that the account number cannot be identified on any carbons that may be discarded after a sales Transaction is completed. The following types of formsets are examples that comply with this rule:

Formset Specifications

B.1.6 Registration Mark

- Carbonless formsets
- Carbon on the back formsets
- Formsets with carbons that are perforated in such a manner that no complete account number remains on the carbon to be discarded

B.1.6 Registration Mark

If the interchange copy of an 80-column formset has a registration mark, then the registration mark must be preprinted and of uniform density of non-reflective (preferably black) ink. The stroke width of the mark must be 0.030 inches \pm 0.010 inches (0.0762 cm \pm 0.0254 cm), and the length of each leg of the mark, measured on its inner edge, must be at least 0.400 inches (1.017 cm). The mark must be aligned with the aligning edge with no visible skew (\pm 2 degrees).

B.1.6.1 Registration Mark Location

If the interchange copy of an 80-column formset has a registration mark, then the location of the registration mark in relation to the leading and aligning edges cannot vary from document to document more than \pm 0.050 inches (\pm 127 cm). The leading edge of the vertical leg of the registration mark shall be 2.40625 inches (6.116 cm) from the left edge of the interchange copy (with the stub removed) and the bottom edge of the horizontal leg shall be 0.625 inches (1.589 cm) from the bottom edge.

B.1.7 Formset Numbering

Each Acquirer must supply its Merchants with consecutively pre-numbered formsets with sequential reference numbers. Each reference number must consist of seven digits, with the seventh digit from the right being a Transaction code (the number “5” on retail sale slips, the number “6” on credit slips, and the number “7” on cash disbursement slips), and must be in 7B font with nominal horizontal spacing of seven characters to the inch.

B.1.7.1 Formset Number Location

On an 80-column Card size formset, the sequential reference number must be located in the 0.500 inches (1.271 cm) clear band area at the top front of each copy of the form. The first (or low order) digit of the reference number must be a minimum of 1.4375 inches (3.653 cm) from the right-most edge of the formset to the beginning of that character; the seventh (or high order) digit must be a maximum of 2.625 inches (6.672 cm) from the right-most edge of the formset to the end of that character; and the centerline of the numbers must be 0.219 inches \pm 0.040 inches (0.557 cm \pm 0.102 cm) from the top of the formset.

B.1.8 Information Slip Specifications

Information slips provide the Cardholder with additional details related to a retail sale, credit, or cash disbursement Transaction. The information slip must be the same size, weight, and color as all other MasterCard formsets.

B.2 Formset Printing Standards

The Standards listed below apply to the printing of formsets.

B.2.1 Retail Sale, Credit, and Cash Disbursement Formsets

This section applies to the printing of the interchange copy of the MasterCard Card formsets for retail sale, credit, and cash disbursement Transactions. Refer to section B.1.8 for printing requirements specific to information slips.

1. The reverse side of any interchange copy shall be blank.
2. The space reserved for imprinting on the interchange copy must remain clear of any printing. This space shall be not less than 3.125 inches (7.943 cm) long by 2.125 inches (5.401 cm) high lying horizontally across the top and commencing at the upper left-hand corner (with the stubs removed).
3. The interchange copies of formsets must have an area not less than 4.250 inches (10.802 cm) long and 0.500 inches (1.271 cm) high lying horizontally across the bottom and commencing at the lower right-hand corner, left clear of any printing.
4. This area shall be not less than 4.500 inches (11.437 cm) long and 0.625 inches (1.589 cm) high, and the balance of the area within 0.625 inches (1.589 cm) of the bottom shall be left clear of any magnetic ink character recognition (MICR) and OCR active printing or markings with the exception of MICR encoding.
5. The interchange copies of formsets must have an area not less than the length of the slip by 0.500 inches (1.271 cm) high lying horizontally across the top of the slip, left clear of any preprinting except for the sequential reference number on an 80-column slip and also discretionary data (located between 0.375 inches and 1.3125 inches [0.953 cm and 3.3359 cm] from the right-hand edge in 7B font).
6. If the formset has a registration mark, a square, formed by a clear band 1/8 inches (0.318 cm) from the external edges and tips of a minimum length registration mark and not less than 11/16 inches by 11/16 inches (1.747 cm x 1.747 cm), shall be left clear of any printing except for the registration mark.
7. The printing on the face of the copies of credit slips shall be in red ink. The printing on the face of the copies of retail sale and cash disbursement slips must not be in red ink. MasterCard recommends that the printing on retail sale slips be in either blue or black ink and on cash disbursement slips in either green or black ink.

B.2.2 Information Slip Formsets

Following is a list of requirements for printing information slips:

1. The following areas shall be left clear of printing:
 - 0.500 inches (1.271 cm) high lying horizontally across the entire length of the top of the slip.
 - 4.500 inches (11.437 cm) long by 0.625 inches (1.589 cm) high lying horizontally across the bottom of the slip commencing at the lower right-hand corner.
 - 1.344 inches (3.415 cm) long by 0.375 inches (0.953 cm) high lying horizontally starting 4.875 inches (12.390 cm) from the left edge and 0.970 inches (2.468 cm) from the top edge of the slip.
 - 0.875 inches (2.224 cm) long by 0.375 inches (0.953 cm) high lying horizontally starting 6.219 inches (15.805 cm) from the left edge and 0.970 inches (2.468 cm) from the top edge of the slip.
 - 6.156 inches (15.647 cm) long by 0.375 inches (0.953 cm) high lying horizontally starting 0.375 inches (0.953 cm) from the left edge and 2.281 inches (5.798 cm) from the top edge.
 - 1.250 inches (3.177 cm) long by 0.375 inches (0.953 cm) high lying horizontally starting 6 inches (15.250 cm) from the left edge and 2.281 inches (5.798 cm) from the top edge.
2. MasterCard recommends using black ink for all printing.
3. For Transaction date identification, the information slip must contain a computer-printed date area. Enter the elements of the date in this area by indicating the sequence (for example, month-day-year) in English and, at the Acquirer's option, also in the local language.
4. For situations when the Transaction date is not available, each information slip will be preprinted with the expression, "Transaction date not available" in English and, at the Acquirer's option, also in the local language.
5. The reverse side shall be blank.

B.2.3 Imprinters

Each Customer is responsible for supplying to its Merchants, on such terms as may be agreed upon between them, and for maintaining at each location disbursing interchange cash disbursements, imprinters capable of producing a satisfactory imprint from a Card upon the interchange copy of a formset. The imprinter must contain a plate that will imprint on the interchange copy of the formset the name and number of the Merchant, or the name of the Customer disbursing the cash disbursement, and the city and state (or country, if the location is outside the United States) where the Transaction occurred.

Appendix C Omitted

This chapter has been omitted.

Appendix D Omitted

This chapter has been omitted.
