MasterCard International

Information about this Replacement

Replacement

The September 2005 *Merchant Rules Manual* replaces your existing manual.

What is in the new version?

This manual contains excerpts of MasterCard member publications that provide information about standards applicable to MasterCard merchants.

Questions?

If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk. If you are a merchant, please contact your acquirer.

MasterCard is Listening…

Please take a moment to provide us with your feedback about the material and usefulness of the *Merchant Rules Manual* using the following e-mail address:

publications@mastercard.com

We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.

MasterCard International

Merchant Rules Manual

September 2005

Copyright

Trademarks

Media

This document is available:

- On MasterCard OnLine®
- On the *MasterCard Electronic Library* (CD-ROM)
- On www.mastercardmerchant.com

MasterCard International Incorporated
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

1-636-722-6100

www.mastercard.com

Chapter 1 Overview

Chapter 2 Excerpts from *Bylaws and Rules* (published April 2005)

Chapter 4 Excerpts from *GCMS Reference Manual* (published May 2005)

Chapter 5 Excerpts from *Security Rules and Procedures* (published July 2005)

Chapter 6 Excerpts from *Maestro Global Rules* (published July 2005)

1 Overview

This chapter provides information on the purpose, audience, and contents of this manual. It also contains important notices regarding the use of this manual.

Purpose

The MasterCard *Merchant Rules Manual* provides merchants with MasterCard rules applicable to merchant acceptance of MasterCard cards and Maestro cards. MasterCard believes that merchants are important participants in the MasterCard and Maestro payment programs and are vital to the continued success of the MasterCard and Maestro brands. MasterCard also believes that merchants and consumers benefit if merchants have access to, and are encouraged to be aware of and conform to, rules that pertain to merchants' acceptance of MasterCard cards and Maestro cards.

A MasterCard member is obligated at all times to comply with MasterCard rules and to cause any merchant from which it acquires MasterCard transactions to at all times comply with MasterCard rules. A MasterCard member may require a merchant to adhere to additional and/or more stringent standards than MasterCard rules require.

Audience

MasterCard provides this manual for the benefit of any merchant that has entered into or is contemplating entering into an agreement with a MasterCard member for the purpose of accepting either MasterCard cards, Maestro cards, or both.

This document is available via the following Web sites:

- www.mastercardonline.com
- www.mastercardmerchant.com

Contents

The manual contains excerpts from the following MasterCard manuals:

Excerpted Manual	Description of Excerpt
Bylaws and Rules published April 2005	The portions of the *Bylaws and Rules* manual included in this *Merchant Rules Manual* address procedures governing the acceptance of MasterCard cards by merchants. Those procedures address such matters as use of the MasterCard marks, prohibited practices such as setting minimum or maximum purchase amounts, merchant obligations such as the obligation to honor all MasterCard cards without discrimination, the authorization and presentment of transactions, and the importance of treating securely card account and transaction data.
Chargeback Guide published May 2005	The portions of the *Chargeback Guide* included in this *Merchant Rules Manual* address procedures governing the acceptance of MasterCard cards by merchants, such as how to complete the sales transaction, deal with suspicious cards, and handle credits and returns, and special procedures that pertain to particular types of transactions, including hotel/motel, cruise line, and car rental transactions.
GCMS Reference Manual published May 2005	The portions of the *GCMS Reference Manual* included in this *Merchant Rules Manual* address cardholder-activated terminal requirements and acceptance procedures governing the treatment of unique transactions and Payment Transactions.
Security Rules and Procedures published July 2005	The portions of the *Security Rules and Procedures* manual included in this *Merchant Rules Manual* address certain responsibilities of a MasterCard member, particularly those regarding any merchant from which the member acquires MasterCard transactions. The included portions also describe programs that MasterCard administers, such as merchant audit, monitoring and registration to ensure that its members and merchants are acting in an appropriate fashion so as to protect cardholder information and reduce chargebacks and fraud.
Maestro Global Rules published July 2005	The portions of the *Maestro Global Rules* manual included in this *Merchant Rules Manual* address procedures for the acceptance of Maestro cards by merchants.

Excerpted Manual	Description of Excerpt
Cirrus Worldwide Operating Rules published June 2005	The portions of the *Cirrus Worldwide Operating Rules* manual included in this *Merchant Rules Manual* address procedures for the acceptance of Cirrus cards by merchants.

Important Notices

The following information contains important notices regarding the use of this text.

- **Excerpted Text.** This *Merchant Rules Manual* consists entirely of text excerpted from other MasterCard manuals as published on the dates noted. The text of the sundry MasterCard manuals is amended from time to time, as requirements are added, deleted, and modified. While we will endeavor to keep the text appearing in this *Merchant Rules Manual* current, in the event of a discrepancy between text set forth in this *Merchant Rules Manual* and the referenced source document, the text set forth in the referenced source document shall be afforded precedence. Because only excerpts of text of manuals are included in this *Merchant Rules Manual*, a reader may not be afforded a complete or accurate understanding of a subject that is referenced or addressed. Merchants should direct any questions to its acquiring or prospective acquiring member.
- **MasterCard International.** MasterCard International ("MasterCard") is a leading global payment solutions company that manages a family of well-known, widely accepted payment card brands, including MasterCard, MasterCard Electronic, Maestro and Cirrus, which MasterCard licenses to its member. The principal members of MasterCard and its affiliates are approximately 2,600 financial institutions worldwide that participate in MasterCard payment programs. In addition, there are over 22,000 affiliate members of MasterCard that participate indirectly in MasterCard payment programs through one or more principal members. MasterCard is structured as an open bankcard association in which cardholder and merchant relationships are managed principally by the members.

- **MasterCard Rules.** MasterCard business is managed by or under the direction of a board of directors and MasterCard rules are approved by that board or pursuant to authority delegated by that board. MasterCard rules are applicable to MasterCard members. If a member acquires MasterCard-branded transactions from a merchant, MasterCard rules will impact how that merchant conducts business. Each MasterCard member is obligated to conduct MasterCard activity in compliance with applicable MasterCard rules and law and to protect, indemnify and hold harmless MasterCard and other members with respect to any claim, demand, loss, cost, liability and/or expense resulting from the member's (and its affiliate members') MasterCard activity and compliance with MasterCard rules.

For the reasons set forth above, any person that uses this *Merchant Rules Manual* or any portion thereof does so at his or her exclusive risk and with the express understanding that MasterCard makes no representations or warranties of any kind whatsoever as to the accuracy or completeness of the text set forth in this *Merchant Rules Manual*.

2 *Excerpts from* Bylaws and Rules *(published April 2005)*

This chapter contains excerpts of the Bylaws and Rules *manual published April 2005. This* Merchant Rules Manual *contains only information that applies to merchants; therefore, some numbered sections provided in the* Bylaws and Rules *manual that do not apply to merchants may have been omitted herein.*

Definitions

The following terms used in this rules portion of the MasterCard International *Bylaws and Rules* manual have the meanings set forth below.

acquirer

As used herein, "acquirer" means a member of the Corporation in its capacity as an acquirer of a MasterCard transaction from a merchant.

approval or approved

As used herein, "approval" or "approved" means the affirmative written approval of the Corporation or its Board of Directors (as applicable), which may be granted, denied, or withheld as conditioned in the Board's or Corporation's sole and absolute discretion.

Board, Board of Directors

As used herein, "Board" or "Board of Directors" means the Board of Directors of MasterCard International Incorporated.

Corporation

As used herein, "Corporation" means MasterCard International Incorporated.

issuer

As used herein, "issuer" means a member of the corporation in its capacity as an issuer of a MasterCard® card or MasterCard account.

Marks

As used herein, "Marks" means the names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks that the Corporation and/or its affiliates or subsidiaries own, manage, license, or otherwise control and make available for use by members and other authorized entities. A "Mark" means any one of the Marks.

member, membership

As used herein, "member" generally means a card member of the Corporation as set forth in Section 3(b) of Article I of the bylaws of the Corporation. Depending on the context, "member" may sometimes mean any member of the Corporation as set forth in the bylaws. As used herein, "membership" means membership in the Corporation and "principal member," "association member," and "affiliate member" mean "principal card member," "association card member," and "affiliate card member," respectively.

sponsorship

As used herein, reference to a member that "sponsors" or "is sponsored by" another member means the relationship set forth in the Standards between a principal or association card member and an affiliate card member.

Standards

As used herein, "Standards" means the bylaws, rules and policies, and the operating regulations and procedures of the Corporation, as may be amended from time to time.

Introduction

These rules set forth and explain certain powers, rights, duties and the responsibilities of MasterCard International Incorporated (referred to in these rules as either "MasterCard" or the "Corporation") and its members in respect to interchange of credit and debit card privileges and the procedures that apply to such interchange, standards for membership, and security safeguards and procedures. Other powers, rights, duties, and responsibilities may be found in the MasterCard Certificate of Incorporation and bylaws.

A fundamental purpose of the Corporation is to provide to the cardholders of its members a means whereby they may enjoy the benefits of full and unrestricted interchange. In furtherance of this end, each member of this Corporation subscribes to the policy adopted by the Board of Directors that it will in good faith use its best efforts to issue the largest number of interchangeable credit and debit cards consistent with sound credit judgment. Each member of this Corporation also undertakes to use its best efforts to participate fully in interchange operations and to implement this Corporation's rules in a manner that will promote complete interchange and that will assure the acceptance of interchange credit and debit cards when properly presented.

The basic purpose of the Corporation is to provide to its members the advantages of widespread interchange while modifying each member's local operations as little as possible. In keeping with this philosophy, the specifications as to forms and procedures contained in these rules are considered to be the minimum standards necessary to make credit and debit interchange workable.

These rules are intended to be solely for the benefit of the Corporation and its members.

3.10 Integrity of Brand and Network

No member may place or cause to be placed on any MasterCard card or any MasterCard card acceptance device any information, applications, or products that would in any way, directly or indirectly, diminish or devalue the brand, impair or discourage acceptance or use of MasterCard cards, products, or services, or impair any aspect of MasterCard transactions or network infrastructure. MasterCard shall have the right, in its sole discretion, in the event of violation of this rule, to require and enforce the immediate removal of such information, application, or products, and to impose a monetary penalty within the framework of MasterCard rules. No member may engage in or support any activity that is illegal, that may, in the opinion of MasterCard, damage the good will of MasterCard, or reflect negatively on the MasterCard

brand. A member that engages in repeated or multiple violations of this Standard or other Standards may be subject to sanctions in addition to those that may be provided for a specific violation of a Standard.

3.11 Discounts or Other Benefits at the Point of Interaction

Subject to other MasterCard Standards, a MasterCard card may not access a discount or other point-of-interaction (POI) benefit unless such discount or other POI benefit may be accessed by any valid MasterCard card. In addition, MasterCard prohibits the promotion at the POI of discounts or other POI benefits on transactions effected with a particular MasterCard card.

The following are the only discount practices permitted in conjunction with a particular MasterCard card:

- A discount or other point of interaction benefit accessed after the transaction has been effected (for example, credit on the billing statement, rebates, and so on); and
- A discount or other POI benefit accessed at the time of or after the transaction has been effected by a separate instrument and not by the MasterCard card (for example, a coupon or voucher).

4.1 Definitions

As used in this Trademarks and Service Marks rules chapter, the following terms have the meanings described.

4.1.1 MasterCard Word Mark

The MasterCard word mark is represented by the word "MasterCard" followed by a registered trademark® symbol or the local law equivalent. The Corporation is the exclusive owner of the MasterCard word mark.

4.1.2 MasterCard Brand Mark

The MasterCard brand mark consists of the MasterCard word mark as a custom lettering legend placed within the MasterCard Interlocking Circles Device. The Corporation is the exclusive owner of the MasterCard brand mark.

4.2 The Right to Use the Marks

4.2.1 Licenses

The right to use the Marks is granted to members and other licensees pursuant to the terms and conditions of a license agreement or other applicable agreement, including all addenda, as may be in effect from time to time. Unless an interim license has been granted, the Marks must not be used in any form or manner before:

- issuance of a written license authorizing the use of the Marks; and
- execution of all applicable license addenda.

No additional interest in the Marks is granted with the grant of a right to use the Marks. Any authorized user of the Marks is responsible for all costs and liabilities resulting from or related to its use of the Marks.

Except as expressly provided in the applicable license agreement, all licenses authorizing the use of the Marks are non-exclusive and non-transferable. The rights to use the Marks may be extended by a licensed member pursuant to a member service provider (MSP) or merchant agreement only to the extent that any rights to use the Marks are limited in such agreement and are in accordance with the Standards.

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

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

4.2.2 Protection and Registration of the Marks

Protection of the Marks is vital to the Corporation and all of its members and licensees. Any use of the Marks must not degrade, devalue, or denigrate the Marks or the Corporation in any way.

Each member and other licensee acknowledges the Corporation's sole ownership of the Marks and agrees not to do anything inconsistent with this ownership. All uses of the Marks will inure solely to the benefit of the Corporation.

In addition to the obligation that no Mark may be used without the consent of the Corporation, no member or licensee of the Corporation or of any of its affiliates or any third party entity that the member or licensee employs may register, attempt to register or in any way make use of the Marks, or any mark or term that, in the sole discretion of the Corporation, is deemed to be derivative of, similar to, or in any way related to the Marks on any card, device or other application associated with a payment service that the Corporation deems to be competitive with any program of the Corporation.

Without limitation, the foregoing shall specifically apply to registration or use of marks or terms that incorporate, reference or otherwise may be confused or associated with the Marks and currently or previously licensed, sublicensed (to the extent sublicensing has been previously permitted) or used by principal or affiliate members, their licensees and permittees and their respective successors or assignees (including, without limitation, by virtue of acquisition by merger or otherwise, bankruptcy or voluntary or involuntary winding-up.) Violation of this rule may subject the member or licensee to significant penalties in the discretion of the Chief Executive Officer of the Corporation or such other disciplinary action as the Board deems appropriate.

4.2.3 Misuse of the Marks

Each member and other licensee must promptly notify the Corporation whenever it learns of any misuse of the Marks or of any attempt to copy or infringe any of the Marks.

4.3 General Rules for Use of the Marks

4.3.1 Use of the Marks

The Marks may be used only pursuant to a written license from the Corporation. This provision applies, without limitation, to:

- use of the Marks for advertising or promotional purposes;
- placing orders for card stock or for any other materials containing the Marks;
- displaying the Marks;
- issuing cards;
- signing merchants; and
- distributing or installing merchant decals.

The Marks must be used only to identify and promote programs and services approved by the Corporation.

4.3.2 Compliance

Any use of the Marks must comply with the applicable license agreement, the Standards, and all of the Corporation's reproduction, usage, and artwork standards as may be in effect from time to time. Any use of the Marks by or on behalf of a member that does not comply with this requirement will be regarded as adequate grounds for expulsion of the member or other disciplinary action deemed appropriate by the Corporation.

4.3.3 Required Uses

Each member must display prominently the Marks in all advertising, marketing, promotional, and collateral materials promoting a program or service offered by the Corporation. The inclusion of the word mark in the headline or title, or the prominent display of the Mark on the first page of the offering, will satisfy this requirement.

4.3.4 Review of Promotional Materials

The Corporation reserves the right to review samples of promotional materials using the Marks. The Corporation promptly will review all submitted materials and notify the licensee as to whether the material complies with the Standards for use of the Marks. Amended samples, if required as a result of this review, also must be forwarded to the Corporation for review.

4.3.5 Signage System

The Corporation's Interlocking Circles Signage System is employed when one or more brands using the MasterCard interlocking circles device is accepted at a point of interaction. The system requires the consecutive vertical or horizontal display of the brand marks in the following sequence—MasterCard, MasterCard Electronic, Maestro, Mondex, Cirrus. Of the five brands, only those brands that are accepted at a particular point of interaction may be displayed. The MasterCard Electronic brand mark must not be displayed on an ATM.

4.3.6 Particular Use of the Marks

4.3.6.1 Use of "MasterCard" in a Corporate or Business Name

The word "MasterCard" must not be used as part of a legal, corporate, or business name, such as "MasterCard Center, Inc."

4.3.6.2 Use of Modifiers

A member is permitted to use its name or a geographical designation in conjunction with the word mark. For example: "California MasterCard card program" or "First Issuer MasterCard Department." The Corporation may prohibit the use of a modifier that it determines will impair the distinctiveness of the Marks or create any likelihood of confusion or reflect poorly on the Corporation.

4.3.6.3 Use on Stationery

Subject to the Standards, licensees are permitted to use the Marks on print or electronic stationery, letterhead, envelopes, and the like for the purpose of identifying their MasterCard programs and services. The licensee's name must appear in close proximity to the Mark and the registration notice or the local law equivalent must be used (as in Superior National Bank MasterCard® Card Department).

4.3.6.4 Use on Non-Licensed Goods

The Marks must not be used to create the impression that any good or service offered by the licensee or other authorized user is sponsored, produced, offered, approved, sold by, or otherwise affiliated with the Corporation. Each licensee must ensure that each of its partners, merchants, and other program participants does not apply a Mark to particular goods or services offered for sale. The Corporation must approve in writing any use of the Marks on unlicensed goods before the first use.

4.3.6.5 Use on Checks

The Marks may not be placed on a check, except as allowed by a separate "Master Checking" license agreement.

4.3.7 Use of the Word Mark

4.3.7.1 Use of the MasterCard Word Mark

The MasterCard word mark must appear in English and must be spelled correctly and as one word. The letters "M" and "C" must be capitalized. "MasterCard" must not be abbreviated, hyphenated, used in the plural or possessive, or translated from English into another language.

4.3.7.2 Generic Use

A generic term such as "bank card" or "payment card" cannot function as a mark. Generic use of a Mark is prohibited because it can result in the loss of trademark rights.

4.3.7.3 Use of "Master" Terminology

To avoid the likelihood of confusion and the loss of distinctiveness of the Marks, and except as expressly permitted by the Corporation, no member, licensee, or authorized user may use the word "Master" as part of a trademark, service mark, corporate name, business name, or program name, whether preceding, following or linked together as one word, or with a hyphen or slash, or in connection with any financial or bank-related goods or services.

4.3.7.3.1 Use of MasterCard in Text

The word "MasterCard" must be used as an adjective (as in "your MasterCard card" or "the MasterCard Brand Mark") in the first or most prominent use of the word mark subsequent to any use in the title, headline, signature, or cover page of an offering, unless:

- the word "MasterCard" is used as part of a member's program name (as in "member/program name MasterCard"); or
- otherwise expressly approved in writing by the Corporation.

Use of the MasterCard word mark as a verb ("MasterCard your gifts"), in plural ("MasterCards") or in possessive form is prohibited.

4.3.7.4 Registration Notice

The MasterCard word mark must be accompanied by the registration notice ® or the local law equivalent. (Refer to the reproduction, usage, and artwork Standards for the correct use and placement of the registration mark.)

4.3.7.5 Program Names

All MasterCard program names, offerings, and services must be referred to by their full, legal name and include the appropriate registration notice.

4.3.8 Use of the Interlocking Circles Device

4.3.8.1 Variations Prohibited

All modifications, alterations, and variations of the Corporation's interlocking circles device are prohibited, except as expressly permitted by the Corporation.

4.3.8.2 Standard Colors

The interlocking circles device must be reproduced in accordance with all color and version specifications as set forth in the MasterCard International Brand Center Web site at www.mastercardbrandcenter.com and the *Card Design Standards Manual*.

4.3.8.3 Legends

The interlocking circles device always must have a MasterCard brand name in custom lettering placed within the circles as specified within the Brand Center Web site at www.mastercardbrandcenter.com, except as expressly permitted by the Corporation. Only a permitted MasterCard brand name, such as "MasterCard," "MasterCard Electronic," "MasterCard Maestro," "Maestro," "Mondex," or "Cirrus," accompanied by the appropriate registration notice, may be superimposed on any part of the interlocking circles device.

4.3.8.4 Registration Notice

The interlocking circles device must be accompanied by the registration notice ® or the local law equivalent close to the Mark. If the maximum horizontal dimension of the interlocking circles device is one inch or less, the registration notice may be omitted.

4.3.8.5 Use of Similar Logos, Designs, and Names

A member, licensee, or other authorized user must not use any logo, design, or decorative element that includes two or more interlocking, adjoining, or adjacent circles, spheres, globes, or similar shapes that could cause confusion with, or dilute the distinctiveness of, the interlocking circles device.

4.3.9 Use of Multiple Brand Marks

4.3.9.1 Parity

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

When promoting the Marks with other acceptance marks, in any media including print, electronic advertising, promotional literature, signs, decals, and any other graphic image used to indicate acceptance, no other acceptance mark, symbol or logo may be of a greater dimension than, or in any way be larger than or appear to be more important than or more welcomed than, the Marks.

- To maintain visual parity, the Marks must be at least as prominent as, and appear in at least the same frequency, size, and color treatment as, all other acceptance marks displayed, as specified in the Brand Center Web site at www.mastercardbrandcenter.com.
- To maintain parity within written text, the word marks must be at least as prominent as, and appear at least as frequently as, any other acceptance mark mentioned.

4.3.10 Use of the Card Face Design

4.3.10.2 In Merchant Advertising

Merchants are prohibited from using the MasterCard card face design to indicate acceptance in merchant advertising or in point-of-interaction ("POI") materials, including use of the MasterCard card face design on any signage, decal, or graphic image at a physical or electronic point of interaction. A merchant is permitted to display an issuer-specific card face design in merchant advertising and POI material provided that it is not used to signify acceptance.

4.4 Additional Requirements for Acquirers and Merchants

4.4.1 Merchant Agreement

A merchant is only permitted to use the Marks pursuant to the merchant agreement with its acquirer. The merchant agreement must include provisions stating that:

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

The acquirer must ensure that its merchant uses or displays the Marks in accordance with the Standards.

The acquirer must ensure that its merchant ceases all use of the Marks and promptly returns any materials displaying the Marks immediately upon termination of the merchant agreement or notification by the Corporation to discontinue such use.

The use or display of the Marks does not give a merchant any ownership or interest in the Marks.

4.4.1.1 Direct Mail Cardholder Solicitation Merchants

Each merchant agreement with a Direct Mail Cardholder Solicitation Merchant shall contain the following provision:

"Merchant acknowledges that the trademark 'MasterCard' and the corresponding logotype are the property of MasterCard International Incorporated. Merchant shall not infringe upon the mark or logo, nor otherwise use the mark or logo in such a manner as to create the impression Merchant's goods or services are sponsored, produced, affiliated with, offered, or sold by this Corporation.

"Merchant shall not use the mark or logo on its stationery, letterhead, envelopes, or the like nor in its solicitation; provided, however, that Merchant may use one of the mark or logo in close proximity to the payment or enrollment space in the solicitation in a size not to exceed 1 1/4 inches in horizontal length if a logo is employed, or, if a mark is used, in type not to exceed the size of the type used in the major portion of the text on the same

page; provided further that the legend, 'Accepted for Payment' must accompany the mark or logo used and must be the equivalent size of the mark or logo. In no case, however, shall Merchant use any of the logo on the front or first page of its solicitation. One truthful statement that Merchant is directing or limiting its offer to MasterCard cardholders may appear in the body of the solicitation, other than in close proximity to the payment or enrollment space, subject to the limitation that: (1) only the word mark may be used; (2) the word mark may not (a) exceed in type size the size of any other type on the same page, (b) differ in color from the type used in the text (as differentiated from the titles) on the same page, (c) be as large or as prominent as the name of Merchant, (d) be the first item appearing on any page, nor (e) in any other way be the most prominent element of the page; (3) Merchant's name and/or logo must appear prominently on the same page as the mark; and (4) the following disclaimer must appear in close proximity to the mark on the same page and in an equal size and type of print:

'MasterCard International Incorporated is not affiliated in any way with [Merchant] and has not endorsed or sponsored this offer.'

"Merchant further agrees to submit its first direct mail solicitation(s), prior to mailing, to the MasterCard Law Department, to be reviewed only for compliance with this Corporation's trademark rules and shall furthermore not distribute in any manner such solicitations until Merchant shall have obtained this Corporation's written approval of the manner in which it uses MasterCard mark and logo on such solicitations. Merchant shall likewise, upon request, submit to the Corporation any amended solicitations prior to mailing."

4.4.2 Use of the Marks by Merchants

4.4.2.1 Merchants Must Display the MasterCard Brand Mark

Only the MasterCard brand mark may be displayed to indicate acceptance on any point-of-interaction signage. An acquirer must ensure that all of its merchants prominently display the MasterCard brand mark at the point of interaction to indicate that the merchant accepts MasterCard cards.

An acquirer must ensure that each of its remote services merchants display the MasterCard brand mark wherever payment options are presented. Acquirers must provide their merchants with the appropriate artwork in a format authorized by the Corporation.

The MasterCard brand mark must be clearly visible to the public. The preferred location to post the MasterCard brand mark at a physical point of interaction is the entrance, nearby window or door of the merchant or business location, and on the first screen of an electronic point of interaction. Where it is not possible to post signage at the entrance of the merchant or

business location, posting the MasterCard brand mark so that it can easily and readily be seen within the location will satisfy the above requirement. Where it is not possible to post the MasterCard brand mark on the first screen of an electronic point of interaction, posting the MasterCard brand mark on the payment screen will satisfy this requirement.

4.4.2.2 Merchant Advertising and POI Materials

Merchants are permitted to use the MasterCard brand mark in merchant advertising, promotional materials, and images displayed at the point of interaction, including an electronic point of interaction to indicate acceptance.

Other acceptance marks, symbols, logos, or combinations thereof may appear in the same advertising material, POI promotional material, or image with the MasterCard brand mark, if no other acceptance mark, symbol, or logo is more prominent or likely to cause confusion concerning the acceptance of MasterCard cards.

4.4.2.3 Local/Regional Acceptance Brands

The MasterCard brand mark must be displayed as a free-standing mark, and, as such, may not be displayed so as to suggest that it is either a secondary means of payment to a local/regional acceptance brand, or exclusively linked to a local/regional acceptance brand.

Visual parity must be maintained between the MasterCard brand mark and any local/regional acceptance mark also displayed at an acceptance location or in merchant advertising.

6.1 Applicability of the Standards

The rules set forth in Part I of this rules chapter 6 apply to all MasterCard® Affinity/Co-Branded Card Programs (hereinafter each referred to as an "A/CB program"). An A/CB program involves the placement of a trade name, mark, or both, of any entity or group not eligible for membership in the Corporation (the "A/CB partner") on a MasterCard card. The intent of these A/CB rules is to prevent an A/CB partner from enjoying the benefits of membership without being a member.

6.5 Acceptance Requirements

6.5.1 Accept All Cards without Discrimination

Subject to the Standards, each participating merchant must accept MasterCard cards universally. Therefore, a merchant that accepts an A/CB MasterCard card, including a merchant owned or controlled by an A/CB partner, must accept all other MasterCard cards, without limitation or exception.

6.5.2 Use of the MasterCard Mark

The MasterCard brand mark must be displayed on a stand-alone basis apart from any A/CB partner identification at any point of interaction that accepts MasterCard cards. The MasterCard brand mark displayed at the point of interaction must at least have parity in size and prominence with any A/CB logo, program name, and competing payment systems mark also displayed. The Corporation has the right to require the modification of any POI display of an A/CB program name or logo that the Corporation determines does not comply with this rule or adversely affects the MasterCard brand.

The A/CB program MasterCard card face design may not be used as an element of any POI merchant decal.

8.1 Cash Disbursements May Be Provided Only By Members

Cash disbursements may be provided only by members at their facilities and through their authorized agents. For purposes of this rule, an authorized agent is a financial institution authorized to provide cash disbursement services on behalf of a member pursuant to written agreement with the member.

9.1 Signing a Merchant

9.1.1 The Merchant Agreement

Each member must directly enter into a written merchant agreement with each merchant from which it acquires transactions.

A member shall not submit into interchange any transaction arising in connection with any commercial entity that makes goods or services available to MasterCard cardholders for purchase with a MasterCard® card, unless the commercial entity has a valid merchant agreement with the member. This rule applies regardless of whether the ability to use the MasterCard card is explicit or implied, or whether the MasterCard card is presented directly to the commercial entity, a third-party payment facilitator, or any other person. A commercial entity is any person that sells goods or services on an ongoing basis and that maintains a physical or virtual presence for the purpose of selling goods or services. This rule does not prohibit a commercial entity from being the recipient of funds that result from a MasterCard money transfer transaction, provided the transaction is properly identified as such to the issuer and cardholder with the appropriate merchant category code (MCC) and transaction category code (TCC) in all authorization and clearing records.

9.1.1.1 If Using an MSP

Regardless of whether a member uses a Member Service Provider ("MSP"), the member must itself execute a written agreement directly with each merchant. The agreement must reflect the member's primary responsibility for the merchant relationship and must otherwise comply with the Corporation's Standards.

9.1.2 Required Provisions

Each merchant agreement must contain the substance of each of the Standards set forth in the Merchant Obligations section of this chapter. The failure to include the substance of any one or more of such Standards in the merchant agreement or the grant of a waiver or variation with respect to one or more of these provisions does not relieve a member from chargebacks or compliance proceedings. The merchant agreement may contain other such provisions that may be agreed upon between the member and the merchant, provided that the provisions do not conflict with the Standards.

9.1.3 Member Responsibility for Merchant Compliance

The member is responsible for ensuring that each of its merchants complies with the Standards, including those applicable to unique transactions, cardholder-activated terminals, and the like, and is itself responsible to the Corporation and to other members for the merchant's failure to do so. The member shall take such actions that may be necessary or appropriate to ensure the merchant's compliance, such as reviewing the merchant's deposit records and procedures for effecting MasterCard transactions. Failure to comply with any of the Standards may result in chargebacks, a penalty to the member, or other disciplinary action.

9.2 Before Signing a Merchant

9.2.1 Verify Bona Fide Business Operation

Before entering into, extending, or renewing a merchant agreement, a member must verify that the merchant from which it intends to acquire MasterCard transactions is a bona fide business and that the transactions will reflect bona fide business between the merchant and the cardholder. Procedures for verifying that a merchant will engage in bona fide business are found in section 5.2 of the *Security Rules and Procedures* manual.

These merchant signing Standards do not apply to the extent that compliance would violate local law. The Corporation must be notified promptly if compliance with a Standard would cause a violation of applicable law. In such case, the Corporation may require use of an alternative to the Standard if, at the Corporation's discretion, such alternative may provide substantially the same or similar protection.

9.2.2 Retain Investigative Records

A member 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 the agreement is terminated.

9.3 Ongoing Acquirer Obligations and Activities

9.3.1 Acquiring Transactions

Each member must acquire all transactions properly presented to it from each of its merchants on such terms as set forth in the merchant agreement between them and under MasterCard rules and procedures.

9.3.2 Payments to Merchants

Each member must pay its merchant for all transactions received from the merchant no later than the next business day following the day of receipt. The member may delay payment for only as long as it is necessary to determine the legitimacy of the deposit, within local law or banking regulation. Payment must be made by cash, check or credit to an account designated by the merchant. This requirement shall not apply to transaction amounts withheld by an acquirer, by agreement of the merchant, for chargeback reserve or similar purposes.

9.3.3 Supplying Materials

Each member must ensure that each of its merchants is provided with all materials necessary to effect MasterCard transactions in accordance with the Standards and to signify MasterCard acceptance. These materials may include sales slips, credit slips, terminals, authorization services, MasterCard acceptance displays, and the like.

9.4 Merchant Monitoring

9.4.1 Monitoring Requirements

Each member must monitor each of its merchant's activity on an ongoing basis to deter fraud or other wrongful activity. At a minimum, the member must monitor its merchant's deposits and authorization activity. The member must comply with the monitoring Standards set forth in section 5.3 of the *Security Rules and Procedures* manual.

The Corporation has the right at any time to audit a member's files and to determine if the member is in compliance with the merchant monitoring procedures.

9.4.2 Merchant Standards

The Corporation has established certain Standards applicable to fraudulent transactions and chargeback activity. Members whose merchants exceed or violate these Standards may be subject to fines or other disciplinary action and may be subject to chargeback liability. Standards applicable to fraudulent transactions are set forth in the *Security Rules and Procedures* manual.

9.5 Merchant Noncompliance

9.5.1 Specified Rules Violations

If the Corporation becomes aware that any merchant has violated any of the following rules:

- Honor MasterCard Cards (section 9.11);
- Use of the MasterCard Mark (section 9.10);
- Charges to Cardholders (section 9.12.2);
- Minimum/Maximum Transaction Amount Restrictions (section 9.12.3); or
- Prohibited Transactions (section 9.12.4),

the Corporation will notify the acquirer of the violation and request that it take action to ensure that the merchant discontinues promptly, and in no more than 10 business days, the violative practice. A notification by the Corporation of a violation at any one merchant location requires the member to ensure that the practice is discontinued at all locations covered by the merchant agreement(s).

9.5.2 Assessments

9.5.2.3 Assessments for Disclosure and Securing Account Data Rules Violations

If the Corporation's staff becomes aware of any merchant or any DSE in violation of section 9.15 of these rules, the Corporation may identify and advise the acquirer of such violation, and may impose an assessment for noncompliance of up to USD 100,000 per individual violation, with a maximum aggregate assessment of USD 500,000 for additional or continuing violations during any consecutive 12-month period.

In addition, if a merchant or any DSE is determined to be in violation of section 9.15, or if a member is determined to be in violation of section 3.7 of these rules, and if such violation results in compromised account information, the acquirer must comply with the requirements set forth in section 5.12 of the *Security Rules and Procedures* manual.

9.5.2.4 Terminated Merchants

If a member terminates the merchant agreement with a merchant because of a violation by the merchant of one or more of the rules referenced in section 9.5.1, the member must report the merchant to the MasterCard MATCH™ system within five calendar days of the decision to terminate, regardless of the effective date of the termination. All records of rules violations move with the merchant to any new acquirer. 9.8 Merchant Agreement

Each merchant agreement must contain the substance of these Standards applicable to the nature and manner of the merchant's business. The agreement must reflect that the acquirer has primary responsibility for the merchant relationship and is responsible for ensuring the merchant's compliance with the Standards. The merchant's failure to comply with these provisions may result in a penalty to the member or other disciplinary action.

9.8 Merchant Agreement

Each merchant agreement must contain the substance of these Standards applicable to the nature and manner of the merchant's business. The agreement must reflect that the acquirer has primary responsibility for the merchant relationship and is responsible for ensuring the merchant's compliance with the Standards. The merchant's failure to comply with these provisions may result in a penalty to the member or other disciplinary action.

9.9 Responsibility for Transactions

All merchants are responsible for ensuring that the cardholder understands that the merchant is responsible for the transaction, including the goods or services that are the subject of the transaction, and for related customer service, dispute resolution, and performance of the terms and conditions of the transaction.

9.10 Use of the MasterCard Mark

The merchant's use and display of the Marks must comply with all applicable requirements set forth in chapter 4 of this manual and elsewhere in the Standards.

9.11 Honor MasterCard Cards

9.11.1 Honor All MasterCard Cards

The merchant must honor all valid MasterCard cards without discrimination when properly presented for payment. The merchant must maintain a policy that does not discriminate among customers seeking to make purchases with a MasterCard card. A merchant that does not deal with the public at large (for example, a private club) is considered to comply with this rule if it honors MasterCard cards of cardholders that have purchasing privileges with the merchant.

9.11.2 Cardholder Identification

A merchant must not refuse to complete a MasterCard card transaction solely because a cardholder who has complied with the conditions for presentment of a card at the POI refuses to provide additional identification information, except as specifically permitted or required by the Standards. A merchant may require additional identification from the cardholder if the information is required to complete the transaction, such as for shipping purposes. A merchant in a country or region that supports use of the MasterCard Address Verification Service (AVS) may require the cardholder's ZIP or postal code to complete a cardholder-activated terminal (CAT) transaction, or the cardholder's address and ZIP or postal code to complete a mail order, phone order, or e-commerce transaction.

9.11.3 Electronic Commerce Transactions

A merchant must not refuse to complete an electronic commerce transaction using a MasterCard card solely because the cardholder does not have a digital certificate or other secured protocol.

9.11.4 Scrip-dispensing Terminals

MasterCard cards must not be accepted at terminals that dispense scrip.

9.12 Prohibited Practices

9.12.1 Discrimination

A merchant must not engage in any acceptance practice that discriminates against or discourages the use of MasterCard cards in favor of any other acceptance brand.

9.12.2 Charges to Cardholders

A merchant must not directly or indirectly require any MasterCard cardholder to pay a surcharge or any part of any merchant discount or any contemporaneous finance charge in connection with a MasterCard card transaction. A merchant may provide a discount to its customers for cash payments. A merchant is permitted to charge a fee (such as a bona fide commission, postage, expedited service or convenience fees, and the like) if the fee is imposed on all like transactions regardless of the form of payment used.

- A surcharge is any fee charged in connection with a MasterCard transaction that is not charged if another payment method is used.
- The merchant discount fee is the fee the merchant pays to its acquirer to acquire transactions.

9.12.2.1 Charges for Unique Transactions

A merchant is permitted to charge a fee for a unique transaction in accordance with the Standards found in chapter 4 of the *GCMS Reference Manual*.

9.12.3 Minimum/Maximum Transaction Amount Prohibited

A merchant must not require, or post signs indicating that it requires, a minimum or maximum transaction amount to accept a valid MasterCard card.

9.12.4 Prohibited Transactions

A merchant must not submit for payment into interchange, and a member must not accept from a merchant for submission into interchange, any transaction:

- that represents the refinancing or transfer of an existing cardholder obligation that is deemed to be uncollectible, or
- that arises from the dishonor of a cardholder's personal check, or
- that arises from the acceptance of MasterCard cards at terminals that dispense scrip.

9.12.5 Other Forms of Payment

A merchant must not accept any payment from a customer in any other form (for example, cash or check) with respect to a charge for goods or services that are included on a transaction information document (TID) resulting from the use of a MasterCard card.

9.13 Authorizing Transactions

When required by the Standards or by the acquirer, the merchant must obtain an authorization before completing a transaction. Standards concerning authorizations are set forth in the *Authorization System Manual* and in other manuals. Merchant acceptance procedures are set forth in the *Chargeback Guide*.

9.14 Presenting Transactions

9.14.1 Valid and Invalid Transactions

A merchant must present to its acquirer only valid transactions between itself and a bona fide cardholder.

A merchant must not present transactions that it knows or should have known to be fraudulent or not authorized by the cardholder, or authorized by a cardholder that is in collusion with the merchant for a fraudulent intent. Within the scope of this rule, the merchant is responsible for the actions of its employees.

9.14.2 Present Transactions within Three Business Days

The merchant must present records of valid transactions to its acquirer no later than three bank business days after the date of the transaction, except

- the record must not be presented until after the goods are shipped or the services are performed unless, at the time of the transaction, the cardholder agrees to a properly disclosed delayed delivery of the goods or services,
- when the merchant receives authorization for a delayed presentment (in which case the words "Delayed Presentment" must be noted on the TID),
- when the merchant is obligated by law to retain the sales slip or return it to a buyer upon timely cancellation, in which case the merchant should present the record within 10 business days after the transaction date, and
- when the merchant has multiple locations and uses a central facility to accumulate and present records to the acquirer. In this case, the merchant must present the record in accordance with applicable laws and regulations and, in any event, within 30 days of the transaction date.

9.15 Account, Cardholder, Transaction, and Merchant Information

9.15.1 Sale or Exchange of Account and Cardholder Information Prohibited

A merchant must not sell, purchase, provide, exchange or in any manner disclose MasterCard account number information to anyone other than its acquirer, to the Corporation, or in response to a government request. This prohibition applies to card imprints, transaction receipts, carbon copies, mailing lists, tapes, or other media obtained as a result of a MasterCard card transaction.

9.15.2 Fraudulent or Unauthorized Use of Account Information Prohibited

A merchant must not request or use MasterCard account number information for any purpose that it knows or should have known to be fraudulent or in violation of MasterCard Standards, or for any purpose that the cardholder did not authorize.

9.15.3 Account, Cardholder and Transaction Data Must Be Kept Secure

Merchants and DSEs must keep all systems and media containing MasterCard account, cardholder, or transaction information (whether physical or electronic) in a secure manner so as to prevent access by, or disclosure to any unauthorized party. Merchants and DSEs must destroy all media not necessary to retain, in a manner that will render the data unreadable. Only MasterCard account, cardholder, and transaction information may be stored, and then only to the extent permitted by the Standards.

If an account compromise occurs, the following will apply:

- The merchant must notify the acquirer immediately.
- The acquirer must provide the Corporation with complete information about the account compromise.
- If the account compromise results from the merchant's failure to comply with this rule, the acquirer promptly must engage a data security firm acceptable to the Corporation to assess the vulnerability of the merchant systems and provide the results of such audit (or a forensics examination if required by MasterCard) promptly to the Corporation.
- If the acquirer fails to engage promptly the services of a data security firm acceptable to the Corporation or fails to provide the findings of the audit, or any forensics examination, promptly to the Corporation, the Corporation may assess the acquirer in accordance with the schedule set forth in section 9.5.2 and may assess all investigative costs that the Corporation incurs.
- The acquirer must cooperate, and ensure that its merchant cooperates, with the investigation and resolution of the account compromise, including any forensic audit or other measure that the Corporation deems necessary in its sole discretion.

Refer to section 5.12 of the *Security Rules and Procedures* manual for additional requirements applicable in the event of account data compromise.

9.15.4 Account Information Must Not Be Recorded on a Mailer

A merchant must not ask a cardholder to record a MasterCard card account number or other account information on the exterior of any order form or other similar device designed to be mailed.

9.15.5 Merchant Identification

A merchant must prominently and unequivocally inform the cardholder of the identity of the merchant at all points of interaction so that the cardholder readily can distinguish the merchant from any other party such as a supplier of goods or services to the merchant.

9.15.6 Data Storage Entity (DSE) Identification

The merchant must inform the acquirer promptly of the identity of any DSE that engages, or proposes to engage, in the processing, storage, or both of MasterCard account data for the merchant, whether directly or indirectly, regardless of the manner or duration of such activities.

9.15.7 Storage of Account, Cardholder, and Transaction Data

A merchant and any DSE must not store in any system or in any manner, discretionary card-read data, CVC 2 data, PIN data, Address Verification Service (AVS) data, or any other prohibited information as set forth in the MasterCard Standards including, but not limited to, sections 2.5.5.1.1 and 2.8.2.1 of the *Security Rules and Procedures* manual, except during the authorization process for a transaction, that is, from the time an Authorization Request message is transmitted and up to the time the Authorization Request Response message is received. MasterCard permits storage of only the card account number, expiration date, cardholder name, and service code, in a secure environment to which access is limited, and then only to the extent that this data is required for bona fide purposes and only for the length of time that the data is required for such purposes.

Rules Applicable Only to the Asia/Pacific Region

13.A Asia/Pacific Region Variances to Global Rules

13.A.1 MasterCard Affinity/Co-Branded Card Programs

a. Discounts at the Point of Interaction. The use of an A/CB MasterCard card to activate a discount at the point of interaction that is not available on similar purchases with the use of any other MasterCard card is permitted for transactions effected wholly within the Asia/Pacific region. The determination of whether any such discount practice complies with the Standards is at the sole discretion of the Corporation's staff.

b. Multiple A/CB Partners. For A/CB programs issued by members in the Asia/Pacific region, up to two affinity/co-branded partners' names and/or logos may appear on the face of the card subject to the following conditions:

1. the card design shall comply in all respects with the MasterCard Card Design guidelines
2. the MasterCard mark is not obscured by the proliferation of other names and/or logos and the presence of multiple logos does not in any way damage or impair the strength of the MasterCard brand;
3. the decision as to whether any given card design conforms to these conditions is reserved to the Corporation's staff.

c. Proprietary Account Fees. For A/CB programs issued by members in the Asia/Pacific region that are approved for proprietary account access, any proprietary account fees that may be in effect may be waived on a case-by-case basis at the sole discretion of the Corporation's staff.

Rules Applicable Only to the Canada Region

14.A Canada Region Variances to Global Rules

14.A.1 MasterCard Affinity/Co-Branded Card Programs

The use of an A/CB MasterCard card to activate a discount at the POI that is not available on similar purchases with the use of any other MasterCard card is permitted for transactions effected wholly within the Canada region. The determination of whether any such discount practice complies with the Standards is at the sole discretion of the Corporation's staff.

14.B Additional Canada Region Rules

14.B.2 Canadian Merchant Transactions; Deposit Requirements

In the Canada region, each member of the Corporation that acquires MasterCard transactions from Canadian merchants must have a deposit account for each merchant from which it acquires such MasterCard transactions, and the proceeds of such MasterCard transactions must be deposited by the member in such merchant's deposit account.

Rules Applicable Only to the South Asia/Middle East/Africa Region

16.A South Asia/Middle East/Africa Region Variances to Global Rules

16.A.2 MasterCard Affinity/Co-Branded Card Programs

The use of an A/CB MasterCard card to activate a discount at the point of interaction that is not available on similar purchases with the use of any other MasterCard card is permitted for transactions effected wholly within the SAMEA region. The determination of whether any such discount practice complies with the Standards is at the sole discretion of the Corporation's staff.

Rules Applicable Only to the U.S. Region

17.2 Definitions

Solely for purposes of this chapter 17, unless specifically noted,

a. "MasterCard Business" shall mean activities utilizing, involving, or relating to MasterCard branded products (other than travelers cheques), services, programs, and activities, including any product, service, or program branded with the word "Master" as its prefix or that is identified with the design mark utilizing the word mark "MasterCard" superimposed across the distinctive overlapping and/or interlocking circles devices described in section 4.1 of chapter 4 of the Rules portion of the *Bylaws and Rules* manual.

b. the "Region" shall mean the fifty states of the United States of America and the District of Columbia.

c. a "Regional Member" shall mean any MasterCard member licensed as a principal member, affiliate member, or association member of the Corporation, to engage in MasterCard Business within the Region.

d. a "Regional Principal Member" shall mean a principal member or an association member of the Corporation that is licensed as a Principal Member to engage in MasterCard Business within the Region.

17.C Debit-related Rules

This section applies to Debit MasterCard Cards and other MasterCard cards issued in the Region, by Regional members and presented for payment at merchant locations in the Region. Members and merchants in the Region must continue to comply with the global rules for MasterCard cards issued by members outside of the Region and presented for payment at merchant locations in the Region. MasterCard may fix and impose noncompliance assessments on members for violating the rules as set forth in this section 17.C.

17.C.1 Definitions

Solely for the purposes of this section 17.C,

a. "debit" or "Debit MasterCard Card" shall mean any MasterCard-branded consumer device, program, or card issued in the Region, by a Regional Member, that when presented for payment in the United States, accesses, debits, holds, or settles funds from a consumer's demand deposit or asset account. "Debit" or "Debit MasterCard Card" shall include consumer signature debit programs, stored value programs, prepaid cards, payroll cards, electronic benefit transfer cards, and deferred debit cards that access, debit, hold, or settle funds from the user's demand deposit or asset account less than fourteen days after the date of purchase. "Debit" shall not include any point-of-sale device that accesses, debits, hold, or settles funds from the user's demand deposit or asset account fourteen or more days after the date of the purchase.

b. "other MasterCard card" shall mean any MasterCard-branded device, program, or card that is not defined as "debit" or "Debit MasterCard Card".

17.C.2 U.S. Region Variances to Global Rules

The following rules do not apply to a Debit MasterCard Card or other MasterCard card where PIN is used as the cardholder verification method. For rules relating to such transactions refer to section 17.D herein.

a. **Merchant Acceptance**. Merchants that accept MasterCard cards may choose to accept Debit MasterCard Cards only, other MasterCard cards only, or both Debit MasterCard Cards and other MasterCard cards. Acquirers must advise MasterCard when a merchant in the Region chooses not to accept either Debit MasterCard Cards or other MasterCard cards.

b. **Honor All Debit MasterCard Cards**. Section 9.11.1 is modified to require merchants that choose to accept Debit MasterCard Cards to honor all valid Debit MasterCard Cards without discrimination when properly presented for payment. The merchant must maintain a policy that does not discriminate among customers seeking to make purchases with a Debit MasterCard Card.

c. **Honor All Other MasterCard Cards**. Section 9.11.1 is modified to require merchants that choose to accept other MasterCard cards to honor all other MasterCard cards without discrimination when properly presented for payment. The merchant must maintain a policy that does not discriminate among customers seeking to make purchases with another MasterCard card.

17.C.3 Additional U.S. Region Rules

a. **Required Provisions of the Merchant Agreement**. In addition to the Standards set forth in section 9.1.2, merchant agreements must provide the merchant with the option, and the applicable merchant discount rate for each option, to elect to accept Debit MasterCard Cards only, other MasterCard cards only, or both Debit MasterCard Cards and other MasterCard cards. With respect to any contract existing on or before 1 January 2004, under which a merchant accepts MasterCard-branded cards, merchants may choose to stop accepting Debit MasterCard Cards or other MasterCard cards by providing no less than 30 days advance written notice to their acquirer.

b. **Signage**. Merchants that request signage for the purpose of indicating their acceptance of Debit MasterCard Cards must display such signage for a minimum of three months.

Rules Applicable Only to the Europe Region

18.2 Definitions

Solely for purposes of this chapter 18,

a. "Central Acquiring License" shall mean a license that gives a licensee the right to acquire transactions from merchants located outside its area of use in accordance with section 18.B.5 of this chapter 18.

b. "Centrally Acquired Transaction" shall mean a transaction that is acquired by a member located outside the country in which the transaction took place.

c. "EPS-Net" shall mean the telecommunication network for all information (to transfer funds, authorize transactions, validate, clear, reconcile and settle interchange data) exchanged between issuer and acquirer members. The system processes and transmits both time-critical and non-time-critical data.

d. "European Economic Area" shall mean the following countries: Austria, Belgium, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

e. "European Payment System Services (EPSS)" shall mean the company in charge of operating, developing and maintaining EPS-Net and associated services which enables acquirers and issuers to process interchange transactions.

f. "European Regional Proxy Amount" shall mean that portion of the Global Proxy Calculation for all shareholders of MasterCard Incorporated that is owned by the shareholders of Europe. ("Global Proxy Calculation" shall have the meaning set forth in Article IX of the Share Exchange and Integration Agreement by and among MasterCard Incorporated, the Corporation and Europay International S.A., dated as of 13 February 2002.)

g. "Intracountry Transaction" shall mean a transaction acquired in the same country in which the card is issued.

h. "MasterCard Business" shall mean activities utilizing, involving, or relating to MasterCard-branded products (other than travelers cheques), services, programs, and activities, and to the Marks that the Corporation and its affiliates and subsidiaries own, manage, license, or otherwise control and make available for use by members and other authorized entities. This includes any product, service, or program branded with the word "master" as its prefix or that is identified with the design mark utilizing the word mark "MasterCard" superimposed across the distinctive overlapping and/or interlocking circles devices described in section 4.1 of chapter 4 of the Rules portion of the *Bylaws and Rules* manual.

i. "Non-Intracountry Transaction" shall mean, for central acquiring, a transaction completed at a merchant located outside the country in which the card is issued.

j. "Payment Scheme" shall mean MasterCard Incorporated, including all of its subsidiaries and affiliates, its products and services, the Standards that govern the products and services, and its members.

k. the "Region" shall mean the geographical area described in the appendix of this chapter 18.

l. "Regional Affiliate Member" shall mean an affiliate member of the Corporation that is licensed to engage in MasterCard Business within the Region through a Regional Principal Member or a Regional Association Member.

m. a "Regional Association Member" shall mean an association member of the Corporation that is licensed to engage in MasterCard Business within the Region as an association member.

n. a "Regional Member" shall mean any MasterCard member licensed as a principal member, affiliate member, or association member of the Corporation, to engage in MasterCard Business within the Region.

o. a "Regional Principal Member" shall mean a principal member of the Corporation that is licensed to engage in MasterCard Business within the Region as a principal member.

p. "Regional Shareholder" shall mean a Regional Principal Member or Regional Association Member that is an owner of shares of the Corporation.

q. "Sub-Regional Board" shall mean an advisory group created by the Europe Board that may make designations as described in this chapter 18 or as requested by the Europe Board, discuss regional developments, and provide the Europe Board with regional feedback.

r. "Volume" shall mean the financial value of a group of transactions, as opposed to the number of transactions.

s. "Service fee" shall mean a fee paid by the issuer to the acquirer for the service provided in relation to an ATM or manual cash advance transaction.

In addition, use of the term "present" in this chapter 18, with reference to votes taken at meetings of Regional Shareholders shall include both physical presence and presence by proxy. Use of the term "present" in this chapter 18, with reference to votes taken at Europe Board meetings shall not include presence by proxy.

In addition, the following definitions are solely for the purposes of section 18.B.11 of this chapter:

t. "Controller" shall mean the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

u. "Data Subject" shall mean a cardholder or merchant whose Personal Data are processed by a Member or MasterCard Europe sprl or MasterCard International Inc.

v. "EU Privacy Directive" shall mean directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as may be amended from time to time.

w. "Personal Data" shall mean any information related to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, e.g. by reference to an identification number.

x. "Processor" shall mean the entity which processes Personal Data on behalf of a Controller.

y. "Processing of Personal Data" shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

z. "Transaction Data" shall mean Personal Data required for authorizing, recording, settling and clearing a transaction using a MasterCard card and processed by the Corporation in connection with its card activities (e.g. BIN numbers, ICA number, transaction details, MCC, TCC).

18.A Europe Region Variances to Global Rules

18.A.2 Member Obligations

18.A.2.2 Discounts at Point of Interaction

Section 3.11 of these rules is modified as follows:

A discount may be applied at a POI location upon simple presentation of a particular MasterCard card for payment.

18.A.2.3 Charges to Cardholders

Section 9.12.2 of these rules does not apply in the European Economic Area.

If a merchant applies a surcharge for payment by MasterCard card, the amount of the surcharge must be clearly indicated to the cardholder at the POI location and must bear a reasonable relationship to the merchant's cost of accepting MasterCard cards.

18.A.3 Special Issuing Programs

18.A.3.1 Affinity/Co-Branded Card Programs

Part I of chapter 6 of this manual is modified as follows.

18.A.3.1.1 Definitions

"Affinity Card Program" shall mean a card program that solicits individuals who share common interests, activities, or membership in a specific organization. Many of these organizations (also known as 'Affinity Groups') are non-profit.

"Co-branded Card Program" shall mean a card program that is targeted to the customer base of a merchant, service provider, or other commercial organization. A co-branding partner is typically a profit-based company with a recognized brand or logo. It may have merchant outlets and/or an existing card program.

Cardholder services (for example, assistance services) that are part of a member's standard current account package are not considered to be part of Affinity or Co-branded Card Programs.

18.A.3.1.3 Discounts at Point of Interaction

A discount may be applied at a POI location solely upon presentation of an Affinity/Co-branded card.

18.A.6 Cardholder-Activated Terminals (CATs)

Chapter 4 of the *GCMS Reference Manual* is modified as follows.

18.A.6.1 Self-Service Terminals/Level 2

For Self-Service Terminals/Level 2, the maximum transaction amount is EUR 50.

18.A.6.2 Limited Amount Terminals/Level 3

For Limited Amount Terminals/Level 3, the maximum transaction amount is EUR 50.

18.A.6.3 In-flight Commerce Terminals/Level 4

For In-flight Commerce Terminals/Level 4, gambling transactions are not permitted.

18.A.7 Transaction Processing

18.A.7.1 Transaction Information Documents (TIDs)

In addition to the provisions of section 2.1.6.2.1 of the MasterCard *Chargeback Guide*, two currency denominations may be shown on an electronically-generated terminal receipt, when the transaction amount in a different currency is printed at the bottom of the receipt with a clear indication that it is being provided only for information purposes. A maximum of two currencies may be indicated on an electronically generated terminal receipt.

18.B Additional Europe Region Rules

18.B.8 Transaction Processing

18.B.8.1 Refund Transactions

Refund transactions do not require online/voice authorization.

18.B.11 Data Protection

18.B.11.1 Processing of Transaction Data

With regard to Transaction Data, Members in the European Union must comply with the applicable national legislation implementing the EU Privacy Directive. In this respect, Members are Controllers with regard to the Processing of Transaction Data for the purposes of authorizing, recording, clearing and settling transactions, and MasterCard International Inc. and MasterCard Europe sprl are Processors for these purposes. It is also acknowledged that MasterCard International Inc. and MasterCard Europe sprl act jointly with the Members as Controllers in relation to the processing of Transaction Data for statistical, research and analytical purposes.

MasterCard International Inc. and MasterCard Europe sprl will, to the extent they act as Processors, only undertake Processing of Personal Data in accordance with the Rules and will comply with security obligations equivalent to those imposed on the Members as Controllers by Article 17 of the EU Privacy Directive, as implemented by national legislation.

18.B.11.2 Data Subjects Communications and Consent

Members must ensure that the Data Subjects are properly informed and, if necessary, have given proper consent—in accordance with national legislation, that:

a. Transaction Data relating to them may be processed by MasterCard Europe sprl and MasterCard International Inc. for the purposes of authorizing, recording, clearing and settling transactions and that such data may be used for statistical, research and analytical purposes;

b. Data Subjects can request access to the Personal Data held by the Members, MasterCard Europe sprl or MasterCard International Inc., and require that any inaccurate or unnecessary data is corrected or deleted.

18.B.11.3 Applications from Data Subjects

Members must set up appropriate procedures for dealing with applications for access to, correction and/or deletion of Personal Data from Data Subjects in accordance with national legislation. MasterCard Europe sprl and MasterCard International Inc. will cooperate fully with Members in responding to any such application and will, in particular, provide prompt access to Transaction Data held by them to enable Members to comply with any request for access to such Personal Data.

In case such application is made directly to MasterCard Europe sprl or MasterCard International Inc., Members must co-operate with the Corporation in promptly answering such application.

3 *Excerpts from* Chargeback Guide *(published May 2005)*

This chapter contains excerpts of the Chargeback Guide *published May 2005. This* Merchant Rules Manual *contains only information that applies to merchants; therefore, some numbered sections provided in the* Chargeback Guide *that do not apply to merchants may have been omitted herein.*

2.1 Acceptance Procedures

The following sections contain acceptance procedures excerpted in previous editions from the *Bylaws and Rules* manual; however, effective with the October 2002 edition of the guide, these acceptance procedures were removed from the *Bylaws and Rules* manual and may be found only here.

Note **Members should cite the appropriate section number when filing compliance cases.**

2.1.1 Acceptance Procedures for Purchase Transactions

The following sections contain information and requirements relevant to the card acceptor's acceptance procedures for purchase transactions.

2.1.1.1 Card Must be Present

Members should cite Chargeback Guide 2.1.1.1

A MasterCard card must be presented to the card acceptor for all transactions except in the case of mail orders, phone orders, non–face-to-face unique transactions, e-commerce transactions, and preauthorized orders.

2.1.1.2 Determine whether the Card is Valid

Members should cite Chargeback Guide 2.1.1.2

The card acceptor must complete the following steps to determine whether each card presented is a valid MasterCard card:

- Check the valid date and the expiration date on the face of the card. If the card is expired or not yet valid, the card acceptor must obtain an authorization from the issuer.
- Check the Electronic Warning Bulletin or international Warning Notice(s). If the account number is listed, the card acceptor must not complete the transaction without obtaining an authorization from the issuer.
- Compare the four-digit truncated account number imprinted in the signature panel with the last four digits of the embossed account number on the face of the card.
- Unless a hybrid terminal is used, compare the embossed account number on the face of the card with the number displayed or printed from the POI terminal.

If a photograph of the cardholder is present on the card, compare the photograph on the card with the person presenting the card.

- Check that the card is signed.
- For unique transactions processed in a face-to-face environment (with the exception of truck stop transactions and card-read transactions where a non-signature CVM is used), request personal identification of the cardholder in the form of an unexpired, official government document. Compare the signature on the personal identification with the signature on the card.

2.1.1.3 Unsigned Cards

Members should cite Chargeback Guide *2.1.1.3*

If the card is not signed, the card acceptor must:

- obtain an authorization from the issuer, and
- ask the cardholder to provide identification (but not record the cardholder identification information), and
- require the cardholder to sign the card.

The card acceptor must not complete the transaction if the cardholder refuses to sign the card.

2.1.1.4 Suspicious Cards

Members should cite Chargeback Guide *2.1.1.4*

If the card acceptor believes that there is a discrepancy in the signature, or if the last four digits of the embossed account number do not match the four-digit truncated account number on the signature panel or displayed on the terminal, or if the photographic identification is uncertain, the card acceptor must contact its acquirer for instructions. Card acceptors processing unique transactions via a terminal must follow the procedures described in chapter 4 of the *GCMS Reference Manual*. If any unexpired MasterCard card does not have a MasterCard hologram on the lower right corner of the card face, the card acceptor must pick up the card and contact its acquirer's Code Ten operator to advise it of the pick-up and to receive mailing instructions.

2.1.2 Obtaining an Authorization

The following sections contain information and requirements relevant to the card acceptor's obtaining of an authorization.

2.1.2.1 Treat All Transactions the Same

Members should cite Chargeback Guide 2.1.2.1

With respect to securing authorizations of transactions, an acquirer must treat all transactions at a card acceptor location in the same manner.

2.1.2.2 Retain the Card While Obtaining Authorization

Members should cite Chargeback Guide 2.1.2.2

The card acceptor must use its best efforts, by reasonable and peaceful means, to retain the card while making an authorization request.

2.1.2.3 When to Obtain an Authorization

Members should cite Chargeback Guide 2.1.2.3

A card acceptor must obtain an authorization from the issuer before completing the transaction in the following instances:

- The transaction amount exceeds the card acceptor's floor limit or the floor limit applicable to the transaction.
- The card is expired or not yet valid.
- The card is not signed. (See section 2.1.1.3 of these rules for identification requirements and card acceptor procedures.)
- The card acceptor wishes to delay presenting the transaction record.
- The transaction receipt cannot be imprinted although the card is present.
- The card acceptor's data processing equipment is unable to read the magnetic stripe or the chip (if one is present) on the card.
- The account number is listed on the regional Warning Notice.
- The transaction is a recurring payment and a previous authorization request was declined.
- The card acceptor is suspicious of the transaction for any reason.

2.1.2.4 Reporting a Suspicious Transaction

Members should cite Chargeback Guide 2.1.2.4

To report a suspicious transaction, the card acceptor must contact the authorization center, state "This is a Code Ten" and await instructions. Members in regions other than the U.S. region may adopt a term other than Code Ten for use when a card acceptor is suspicious, subject to the Corporation's approval.

In all instances, except where the transaction exceeds the applicable floor limit, the card acceptor must inform the authorization center of the reason for the authorization request.

2.1.2.5 Pick-Up-Card Response

Members should cite Chargeback Guide 2.1.2.5.

If a cardholder account is listed in on the Electronic Warning Bulletin or regional Warning Notice, the card acceptor must not complete the transaction. The card acceptor must retain the card by reasonable and peaceful means and notify the authorization center for further instructions. If a card acceptor is advised by the authorization center to pick up the card, or is given other instructions, the card acceptor must use its best efforts by reasonable and peaceful means to comply with the instructions. If the authorization center cannot be reached, the card acceptor must retain the card by reasonable and peaceful means until the center can be reached.

2.1.3 Obtaining an Authorization for Hotel/Motel, Cruise Line, and Vehicle Rental Transactions

The following sections contain information and requirements relevant to the card acceptor's obtaining of authorizations for hotel/motel, cruise line, and vehicle rental transactions.

2.1.3.1 Authorization Procedures

Members should cite Chargeback Guide 2.1.3.1.

Hotel, motel, vehicle rental, and cruise line card acceptors must comply with the authorization procedures outlined in section 2.1.2 and the requirements set out below.

2.1.3.2 Initiating the Transaction

Members should cite Chargeback Guide 2.1.3.2.

When the transaction is initiated, the card acceptor must request an authorization for an estimated transaction amount if the estimate exceeds the applicable floor limit. The card acceptor also may request an authorization for any additional estimated amounts as needed.

Card acceptors engaging in vehicle rental transactions may not include charges representing either:

- the vehicle insurance deductible amount, or
- an amount to cover potential damages when the cardholder waives insurance coverage at the time of the rental.

Vehicle rental card acceptors must disclose to the cardholder at the time of the rental the amount for which the authorization was obtained.

Charges for damages must be processed as a separate transaction. The card acceptor must provide a reasonable estimate of the cost to repair the damages and obtain agreement from the cardholder. If the cardholder chooses to pay for the repairs using his or her MasterCard card, the card acceptor must:

- Prepare a specific sales slip with proof of card presence
- Provide the estimated amount for repairs indicating that the amount will be adjusted accordingly pursuant to completion of the repairs and submission of the invoice for such repairs
- Obtain a signature from the cardholder

The final transaction amount may not exceed the card acceptor's estimated amount by more than 15% (or less, as directed by local ordinances). The card acceptor must submit a credit if the final cost of repairs is less than the estimated amount on the sales slip. The card acceptor has 30 days from the date of the subsequent transaction related to damages to submit the item into clearing.

2.1.3.3 Completing the Transaction

Members should cite Chargeback Guide 2.1.3.3

When the transaction is completed (that is, when customer checks out of the hotel/motel or returns the vehicle) and the final transaction amount is determined, the following will apply:

IF...	THEN...
The final transaction amount does not exceed the card acceptor's floor limit	The card acceptor is not required to obtain an authorization, but it must check the account number against the international *Warning Notice* or the Electronic Warning Bulletin.
The final transaction amount does not exceed the card acceptor's estimated amount by 15%	The card acceptor is not required to request a secondary authorization. The initial authorization guarantees the full amount of the transaction.
The final transaction amount exceeds the card acceptor's estimated amount by 15%	The card acceptor must request a secondary authorization on the additional amount.
The final transaction amount exceeds the card acceptor's applicable floor limit, **but** a previous authorization was not received because the card acceptor's estimate did not exceed its applicable floor limit	The card acceptor must obtain an authorization for the full amount of the transaction.

2.1.3.4 Subsequent Authorization Requests

Members should cite Chargeback Guide 2.1.3.4.

If the issuer declines a subsequent authorization request, the card acceptor is guaranteed the cumulative amount of previous authorizations, plus 15%.

If a pick-up-card response is received in response to a subsequent authorization request, the card acceptor must pick up the card. The card acceptor is guaranteed the cumulative amount of the previous authorizations, plus 15%.

2.1.4 Obtaining an Authorization when a Gratuity is Added

The following sections contain information and requirements relevant to the card acceptor's obtaining of an authorization when a gratuity is added, either before or after the authorization process.

2.1.4.1 Authorization Procedures

Members should cite Chargeback Guide 2.1.4.1

The following procedures apply to transactions in which the cardholder adds a gratuity:

IF…	THEN…
The transaction amount is below the card acceptor floor limit, **and** the cardholder adds a gratuity in an amount less than or equal to 20% of the transaction amount	The card acceptor **is not** required to obtain an authorization even though the total transaction amount may exceed the card acceptor floor limit.
A card acceptor obtained an authorization for a transaction, **and** the cardholder adds a gratuity in an amount greater than 20% of the transaction amount	The card acceptor must obtain an authorization for the additional amount. The issuer is responsible for the full amount of the transaction.
The cardholder adds a gratuity in an amount greater than 20% of the transaction amount **and** causes the transaction amount to exceed the card acceptor floor limit	The card acceptor must obtain an authorization for the total amount of the transaction.

2.1.5 Obtaining an Authorization for Chip-Read Transactions

Members should cite Chargeback Guide 2.1.5.

When an authorization from the issuer is required for a chip-read transaction, before completing the transaction the card acceptor must obtain a transaction certificate and related data.

For all non–face-to-face chip-read transactions completed via cardholder-controlled remote devices, the card acceptor must obtain an online authorization and the transaction must be Full Grade. For such transactions, issuers may transmit an Authorization Response Cryptogram (ARPC) with an authorization number instead of the transaction certificate and related data.

2.1.6 Completing the Transaction Information Document (TID)

The following sections contain information and requirements relevant to the completion of the Transaction Information Document (TID).

2.1.6.1 Include All Goods on One TID

Members should cite Chargeback Guide 2.1.6.1.

All goods and services purchased in the same transaction must be included on a single transaction information document (TID).

2.1.6.2 TID Information Requirements

Members should cite Chargeback Guide 2.1.6.2

The information in sections 2.1.6.2.1 through 2.1.6.2.7 must be included on the TID.

2.1.6.2.1 A Description of the Goods

Members should cite Chargeback Guide 2.1.6.2.1

A description of the goods and services and their price, including applicable taxes, must be entered on the TID in detail sufficient to identify the transaction. If no currency is identified on the TID, the transaction is deemed to have taken place in the currency that is legal tender at the point of interaction. If the card acceptor offers multiple currencies, then the TID must indicate all of the following information:

- The transaction amount in the merchant's local currency (the goods or services total);
- The converted transaction amount in the currency chosen and agreed to by the cardholder and the merchant (the sale total);
- The currency symbol of each,
- The method by which the currency agreed to by the cardholder was converted from the amount in the merchant's local currency; and

- Either of the following statements: "I understand that MasterCard has a currency conversion process and that I have chosen not to use the MasterCard currency conversion process and I will have no recourse against MasterCard with respect to any matter related to the currency conversion or disclosure thereof" **or** "I have chosen not to use the MasterCard Currency conversion process and agree that I will have no recourse against MasterCard concerning the currency conversion or its disclosure."

2.1.6.2.2 The Transaction Date

Members should cite Chargeback Guide 2.1.6.2.2.

The transaction date must be entered on the TID.

2.1.6.2.3 An Imprint of the Card

Members should cite Chargeback Guide 2.1.6.2.3.

A legible imprint of the card must be made on the TID, or the card acceptor may electronically record the customer's card information and the card acceptor location.

If a transaction is completed without obtaining a card imprint or electronically derived card information, the card acceptor must note legibly on the sales receipt sufficient detail to identify the cardholder, the card acceptor, and the card issuer. This information must include at least the name and address of the card acceptor, the name or trade name of the issuer as it appears on the face of the card, the account number, the MasterCard security character, the expiration date (or dual date), the cardholder name, and any company name.

If the transaction is completed without obtaining a card imprint or electronically derived card information, the card acceptor is deemed to have warranted the true identity of the customer as the cardholder, unless the card acceptor obtained and noted on the TID independent evidence of the cardholder's true identity.

Transactions based on mail orders, telephone orders, preauthorized orders, electronic commerce orders, MasterCard Guaranteed Reservations and Advanced Resort Deposits may be completed without a card imprint.

2.1.6.2.4 The Authorization Number

Members should cite Chargeback Guide 2.1.6.2.4.

If an authorization is obtained from the issuer, unless the transaction is an offline chip-read transaction, the authorization number must be entered on the TID. If more than one authorization is obtained over the course of the transaction (as may occur for hotel, motel, or vehicle rental transactions), all authorization numbers, the amounts authorized, and the date of each authorization must be entered on the TID.

2.1.6.2.5 The Primary Account Number

Members should cite Chargeback Guide 2.1.6.2.5.

The primary account number (PAN) must be truncated on all cardholder-activated terminal TIDs. Subject to local and national laws, PAN truncation is permitted on any other TID type. The Corporation recommends that only the last four digits of the PAN be printed on the receipt. Truncated digits should be replaced with fill characters such as "x," "*," or "#," and not with blank spaces or numeric characters.

2.1.6.2.6 Delayed Presentment

Members should cite Chargeback Guide 2.1.6.2.6.

When the card acceptor receives approval for delayed presentment, the authorization number and the words "Delayed Presentment" must be noted legibly on the TID.

2.1.6.2.7 Cardholder Identification

Members should cite Chargeback Guide 2.1.6.2.7.

For unique transactions processed in a face-to-face environment (with the exception of truck stop transactions and card-read transactions where a non-signature CVM is used), the card acceptor must record on the TID a description of the unexpired, official government document provided as identification by the cardholder, including any serial number, expiration date, jurisdiction of issue, customer name (if not the same name as embossed on the card), and customer address.

2.1.6.2.8 The Transaction Certificate

Members should cite Chargeback Guide 2.1.6.2.8.

The transaction certificate is not required on the TID. However, if the acquirer elects to record the receipt of a transaction certificate on the TID, then the card acceptor must enter the complete transaction certificate on the TID.

2.1.6.2.9 Prohibited Information

Members should cite Chargeback Guide 2.1.6.2.9.

The TID or any other document must not reflect the following information:

- The PIN, any part of the PIN, or any fill characters representing the PIN
- The card validation code 2 (CVC 2), which is indent-printed on the signature panel of the card

MasterCard prohibits the recording of PIN data and CVC 2 data in any manner for any purpose.

2.1.6.3 Obtain the Cardholder's Signature

Members should cite Chargeback Guide 2.1.6.3.

In a face-to-face environment, the card acceptor must give the cardholder the option of a signature-based transaction. Unless the cardholder uses a PIN, the cardholder must sign the TID.

2.1.6.3.1 Compare Signatures

Members should cite Chargeback Guide 2.1.6.3.1.

Unless the cardholder uses a PIN, the card acceptor must compare the signature on the TID with the signature on the card to determine whether they appear to be the same.

2.1.6.3.2 Discrepancy Between Signatures

Members should cite Chargeback Guide 2.1.6.3.2.

If the card acceptor believes that the signature on the card does not match the signature on the TID, the card acceptor must contact the acquirer for instructions. The signature would not match if the signature panel were signed "Jan H. Hanley" and the sales receipt "Bob Hanley" or "F. Hanley." The signature would be acceptable if signed "Jan H. Hanley," "J. H. Hanley" or "Jan Hanley." The signature would be acceptable if a title such as Mr., Mrs., or Dr. is missing or is included.

2.1.6.3.3 Signature Not Required

Members should cite Chargeback Guide 2.1.6.3.3.

Transactions based on mail orders, phone orders, preauthorized orders, electronic commerce orders, MasterCard Guaranteed Reservations, Advanced Resort Deposits and Express Checkouts may be completed without the cardholder's signature. The card acceptor must type or legibly print on the signature line of the TID the letters "TO", "MO", "PO", "EC", "Guaranteed Reservation/No Show," "Signature on File – Express Check-out," or "Advance Deposit" as appropriate. The card acceptor must retain and make available to the acquirer upon request the cardholder's written request to the card acceptor for preauthorization. The card acceptor must not deliver goods or perform services covered by a preauthorization after receiving notification that the preauthorization is canceled or that the MasterCard card covered by the preauthorization is not to be honored.

2.1.6.3.4 PIN as Substitute for Signature

Members should cite Chargeback Guide 2.1.6.3.4.

At points of interaction where MasterCard authorizes the use of a PIN as a cardholder verification method (CVM), the card acceptor is not required to obtain the cardholder's signature if the cardholder uses a PIN.

The card acceptor must obtain a successful PIN validation when PIN is used at a hybrid terminal as a CVM for credit transactions.

2.1.6.4 Give the Cardholder a Copy of the Receipt

Members should cite Chargeback Guide 2.1.6.4.

The card acceptor must provide the cardholder with a true and completed copy of the TID.

2.1.7 Multiple TIDs and Partial Payment

2.1.7.1 Split Tickets are Prohibited

Members should cite Chargeback Guide 2.1.7.1.

A card acceptor is prohibited from using two or more TIDs, also known as a split ticket, to avoid an authorization request.

2.1.7.2 Include All Goods on a Single TID

Members should cite Chargeback Guide 2.1.7.2.

All goods and services purchased in a single transaction must be included in one total amount on a single TID except in the following instances:

2.1.7.2.1 Multiple Cards are Presented

Members should cite Chargeback Guide 2.1.7.2.1.

More than one card is presented for payment on a single transaction, and an authorization is obtained for the portion of the transaction charged to a MasterCard card.

2.1.7.2.2 Multiple Items are Billed

Members should cite Chargeback Guide 2.1.7.2.2.

Multiple items are purchased and individually billed to the same account, and an authorization is obtained for each item purchased.

2.1.7.2.3 Partial Payment

Members should cite Chargeback Guide 2.1.7.2.3.

A card acceptor is prohibited from effecting a MasterCard card transaction where only a part of the total amount is included on a single TID except in the following instances:

- When the cardholder bills a portion of the transaction amount to a MasterCard card and pays the remaining balance by cash or check.
- When the goods or services will be delivered or performed after the transaction date, one TID represents a deposit, and the second TID represents payment of the balance. The second TID is conditioned upon the delivery or performance of the goods or services.

An authorization must be obtained for the total amount of the transaction if it exceeds the applicable floor limit. The card acceptor must note on the TIDs the words “deposit” or “balance,” as appropriate. The TID representing the balance must not be presented until the goods or services are delivered or performed.

This example is provided for illustration only and is not to be cited as an excerpt from Chargeback Guide 2.1.7.

For example, if a chargeback right is not available, paragraph 2.1.7 "Multiple TIDS and Partial Payment" will address situations where the cardholder has paid a "deposit" for merchandise that was agreed to be picked up at the merchant's location by the cardholder. The cardholder then goes to the merchant location and discovers that the merchant is bankrupt or out of business and the cardholder is unable to receive the merchandise.

2.1.8 Returned Merchandise, Adjustments, Credits and Other Specific Terms of a Transaction

2.1.8.1 Card Acceptor Disclosure of Specific Transaction Terms

Members should cite Chargeback Guide 2.1.8.1.

The card acceptor may impose specific terms governing a transaction. In the event of a dispute, and subject to compliance with other Standards, such specific terms shall be given effect, provided that such specific terms were disclosed to and accepted by the cardholder before completion of the transaction. The card acceptor may impose specific transaction terms by, for example, printing the specific terms on the invoice or TID in close proximity to the cardholder signature line before presenting the invoice or TID to the cardholder for signature. Specific transaction terms also may be disclosed by other means, such as by signage or literature, provided the disclosure is sufficiently prominent and clear so that a reasonable person would be aware of and understand the disclosure before the transaction is completed.

Specific transaction terms may include, for example, such words as "Exchange Only," "In-Store Credit Only" or "Original Packaging Required for Returns." Specific terms may address such matters as late delivery, delivery charges, or insurance charges.

2.1.8.2 Returned Merchandise and Canceled Services

Members should cite Chargeback Guide 2.1.8.2.

A card acceptor is not required to accept returned merchandise or the cancellation of services unless a right of return or cancellation was a condition of the transaction. If the card acceptor agrees to accept merchandise for return or to cancel services, the card acceptor must credit the same account used to purchase the merchandise or service.

If the merchandise or service is purchased with a MasterCard card, upon a partial or entire return of merchandise or cancellation of service, or if the card acceptor agrees to a price adjustment, the card acceptor may not provide a full or partial refund or adjustment by cash or check or by any means other than by a credit to the card account used to purchase the merchandise or service. The cardholder must be provided a copy of the credit receipt.

A cash or check refund is permitted for involuntary refunds by airlines or other carriers or card acceptors only when required by law.

2.1.8.2.1 Credit Receipt Requirements

Members should cite Chargeback Guide 2.1.8.2.1.

The credit receipt must contain the following information:

- the date,
- a description of the returned merchandise, canceled services or adjustment made,
- the amount of the credit, and
- the card acceptor's signature.

2.1.9 Charges for Loss, Theft, or Damage

Members should cite Chargeback Guide 2.1.9.

A charge for loss, theft, or damage must be processed as a separate transaction from the underlying rental, lodging, or similar transaction. The cardholder must authorize the charge after being informed of the loss, theft, or damage.

2.1.10 Acceptance Requirements at Hybrid Terminals

Members should cite Chargeback Guide 2.1.10.

For all chip-read transactions, the card acceptor's hybrid terminal must:

- display to the cardholder all mutually supported application labels or preferred names. Multiple matching applications must be displayed in the issuer's priority sequence;
- allow the cardholder to select the application to be used when multiple matching applications exist;
- display to the cardholder the transaction amount; and
- before the transaction is completed, provide the cardholder with the option of approving or canceling the transaction.

2.1.11 Payment Transactions

Members should cite Chargeback Guide 2.1.11.

A Payment Transaction is a transfer of funds to a MasterCard account via the MasterCard interchange system. A Payment Transaction is not a credit that reverses a previous MasterCard purchase A Payment Transaction only may be effected:.

1. By a member pursuant to a BSA (Business Service Arrangement) agreement; or
2. Pursuant to a MasterCard program; or

3. By a member or non-member as a registered Payment Transaction Provider.

2.1.11.1 Payment Transactions Pursuant to Business Service Arrangements (BSAs)

Members should cite Chargeback Guide 2.1.11.1.

A member that wants to effect a Payment Transaction pursuant to a BSA agreement must comply with all Standards, including the Standards set forth below:

1. The member must comply with the requirements set forth in chapter 6 of the GCMS Reference Manual.
2. The BSA must be agreed to in writing, in advance, by MasterCard.
3. Each Payment Transaction must be identified with the correct MCC(s), as required by the Standards.

2.1.11.2 Payment Transaction Pursuant to MasterCard Programs

Members should cite Chargeback Guide 2.1.11.2.

A Payment Transaction may be effected pursuant to a MasterCard program. Members may participate in MasterCard Payment Transaction programs with the written consent of MasterCard.

2.1.11.3 Payment Transaction Provider (PTP)

Members should cite Chargeback Guide 2.1.11.3.

A Payment Transaction Provider (PTP) does not, as such, sell goods or services, but effects a Payment Transaction. A PTP must comply with the Standards set forth in section 2.1 of this guide. The PTP registration request must establish, to the satisfaction of MasterCard, that a MasterCard member has agreed to be the acquirer of record of Payment Transactions effected by the PTP and fully be responsible to MasterCard and other MasterCard members for such Payment Transactions in full compliance with MasterCard Standards. Except as otherwise set forth herein, each Payment Transaction is subject to the Standards, including the indemnity set forth in rule 1.1 of the *Bylaws and Rules*.

1. MasterCard will identify each PTP as either:
   - PTP—Member Financial Institution-Payment Transaction (MCC 6532)
   - PTP—Merchant-Payment Transaction (MCC 6533)
2. A Payment Transaction must not be effected in a manner that is inconsistent with an expressed cardholder preference.
3. Each Payment Transaction must be authorized separately and distinctly by the issuer of the account to which the funds are to be transferred, and must be identified as a Payment Transaction in the Authorization Request Message/0100.

4. A Payment Transaction must be effected on the date agreed to by the PTP and the person whose account is to be funded.
5. Separate Payment Transaction requests must be effected separately and may not be aggregated as a single Payment Transaction. Conversely, a Payment Transaction may not be separated into two or more Payment Transactions. Each Payment Transaction must be authorized, cleared, and settled distinctly and separately.
6. A Payment Transaction may not be effected for any of the following reasons:
   - to dispense nominal (in the sole judgment of MasterCard) merchant incentives or reward programs;
   - to represent itself as an agent of an issuer for the purpose of accepting or initiating payments to a MasterCard account;
   - to "authenticate" a MasterCard account or a cardholder, for example, by effecting or attempting to effect a Payment Transaction for a nominal amount;
   - to transfer gambling winnings or funds related to chips, currency, or other value usable for gambling that were purchased in connection with gambling;
   - for any illegal purpose or any other purpose deemed by MasterCard to be impermissible; or
   - to transfer the proceeds from a MasterCard transaction to a commercial entity or to another MasterCard merchant.
7. A Payment Transaction must be submitted to MasterCard for clearing within one (1) day of the issuer's approval of the authorization request.
8. Funds for the Payment Transaction must be deemed collected and in the control of the acquirer before the Payment Transaction is submitted into interchange
9. A Payment Transaction only may be reversed for reason of a documented clerical error. In such an event, the error must be reversed within three (3) calendar days of the date the Payment Transaction was submitted into interchange. Reversible clerical errors include, by way of example and not limitation, the erroneous capture of transaction data, a duplicate transaction, or an error caused by the transposition of data.

2.2 Additional Acceptance Information

The following sections provide acceptance information for MasterCard Guaranteed Reservations, Express Checkout, and Advance Resort Deposit services.

Note **Members should cite the appropriate section number when filing compliance cases.**

2.2.1 MasterCard Guaranteed Reservations

Members should cite Chargeback Guide 2.2.1.

If a hotel, motel, or resort is participating in the MasterCard Guaranteed Reservations service for all MasterCard cardholders, the hotel, motel, or resort is obligated to have a room available when the MasterCard cardholder arrives (until checkout time the next day). The cardholder is obligated to cancel a confirmed reservation before 18:00 at the hotel, motel, or resort (card acceptor's local time). Failure to do this will allow the hotel, motel, or resort to charge the cardholder a no-show charge equal to one night's lodging. The following procedure will prevail:

1. If a MasterCard cardholder phones a participating hotel, motel, or resort and wants to guarantee a room with his or her MasterCard card, the reservation clerk explains the terms of the MasterCard Guaranteed Reservations service, specifically including the fact that an authorization check will be made at the time of arrival and the cancellation procedure the cardholder must follow to avoid being charged a no show charge equal to one night's lodging.
2. The clerk takes the cardholder's account number, card expiration date, name embossed on the card, and address; confirms the room rate and location; issues the cardholder a reservation confirmation number; and advises the cardholder to retain it. It is recommended that the hotel, motel, or resort also confirm that guaranteed reservation in writing, advising the cardholder of his or her confirmation number and cancellation procedures.

3. If a cardholder who has guaranteed his or her reservation by use of his or her MasterCard card calls the hotel, motel, or resort to cancel the reservation within the agreed upon period, the hotel, motel, or resort is obligated to cancel the guaranteed reservation and issue the cardholder a cancellation number that is verification that the reservation has been canceled. The cardholder should be advised to retain the cancellation number. It is also recommended that the hotel, motel, or resort confirm the cancellation in writing advising the cardholder of the cancellation number.
4. If a cardholder who has guaranteed a reservation by use of his or her MasterCard card arrives within the specified period (until checkout time the next day), the hotel, motel, or resort is obligated to provide a room.

   If the hotel, motel, or resort is unable to provide a room, the hotel, motel, or resort is obligated to provide at no additional charge a comparable room for one night, transportation to the other lodging and a three-minute domestic or long distance phone call, whichever the cardholder deems necessary to advise of a change of location.
5. Before the cardholder's expected arrival, the hotel, motel, or resort shall prepare a registration card and assign a room number on that card.
6. If the cardholder does not cancel and does not stay at the hotel, motel, or resort, the hotel, motel, or resort may bill the cardholder for one night's room rate. The following procedure should be followed:
   a. The outlet completes a sales ticket filling in the cardholder's name, MasterCard account number, card expiration date, date of no show, assigned room number and card acceptor identification, and writes the words "guaranteed reservation/no-show" in place of the cardholder's signature.
   b. Follow your usual authorization procedures.
   c. Assuming the account is not on the *Warning Notice* (or the Electronic Warning Bulletin file in the United States), if under the floor limit, or authorization has been given, the card acceptor deposits the no-show charge in the usual manner. There are no special deposit requirements imposed on the card acceptor outlet.
   d. The actual no-show registration card, reflecting the assigned room number, shall be retained six months from the date the sales ticket is deposited.
7. Where the account number used to guarantee the transaction that results in a no show was unidentifiable as to a specific issuer or was fictitious, the bearer of the liability will be the acquirer.

8. Where the transaction is identifiable to a specific issuer but is not identifiable to a specific account number within that institution, the bearer of the liability will be the acquirer.
9. MasterCard reserves the right to prevent the acquirer from allowing a specific hotel, motel, or resort to participate in the MasterCard Guaranteed Reservations service where in the opinion of MasterCard management, the hotel, motel, or resort has been abusing the privilege.

2.2.2 Express Checkout

Members should cite Chargeback Guide 2.2.2.

If a card acceptor is participating in the Express Checkout service for all MasterCard cards, the card acceptor must:

1. At the time of check-in, inquire whether the MasterCard cardholder would like to use the Express Checkout service or routinely provide the necessary form (Express Checkout Authorization Form) in its "welcome package."
2. Have the MasterCard cardholder complete and sign the Express Checkout Authorization Form. It is recommended that the Express Checkout Authorization Form minimally include the name, address, and phone number of the hotel, motel, or resort, and space for the cardholder's name, address, room number, cardholder signature, and account number that may optionally be imprinted. The form should state clearly that the cardholder directs the hotel, motel, or resort to charge his or her MasterCard account number for his or her bill and process his or her MasterCard sales ticket without a cardholder signature.
3. Imprint a sales ticket with the cardholder's MasterCard account number, and follow its normal authorization procedures. The "preauthorized order" floor limit of USD 50 does not apply.
4. On the cardholder's departure the card acceptor should complete the sales ticket, indicating the total amount of the bill, and print legibly in the space allotted for the customer's signature the words "signature on file—express checkout."
5. Process the sales ticket in the usual manner. There are no special deposit requirements imposed on the card acceptor outlet.
6. Mail a copy of the itemized bill, sales ticket, and the Express Checkout Authorization Form to the cardholder at the address noted on the authorization form within three business days after the cardholder checks out.
7. Retain and make available to MasterCard and the issuer all pertinent records pertaining to the itemized bill and authorization requests in the event of a dispute.

2.2.3 Advance Resort Deposit

Members should cite Chargeback Guide 2.2.3.

If a hotel, motel, or resort is participating in the Advance Resort Deposit service for all MasterCard cards, the following procedures will apply:

1. If a MasterCard cardholder phones a participating card acceptor or travel agent wishing to make an advance deposit with his or her MasterCard card, the reservation clerk explains the terms of the reservation, cancellation, and refund policy procedure to the cardholder.
2. The reservation clerk takes the cardholder's account number, card expiration date, name, and address and confirms the room rate and location.
3. The reservation clerk is required to confirm the status of the card. The authorization procedure is determined by the location (region) of the lodging facility. The applicable procedure follows.

   a. If the lodging facility is located within the U.S. region, the reservation clerk is required to follow the appropriate authorization procedures to obtain approval for the transaction. If authorization is not obtained, the card acceptor accepts responsibility for the transaction.

   b. For all regions other than the U.S. region, the reservation clerk is required to check the *Warning Notice*. (This may be done subsequent to the phone call.) If the account number is listed in the *Warning Notice*, the reservation clerk should follow the usual procedures provided by the acquirer.

   The reservation clerk is required to call for authorization if the amount of the advance deposit exceeds USD 50. If the result of the authorization call is denial, the outlet must so advise the cardholder.
4. The reservation clerk completes a sales ticket filling in the cardholder's name, MasterCard account number, card expiration date, reservation confirmation number, and MasterCard card acceptor identification and writes the words "advance deposit" in place of the cardholder's signature. It is recommended that the card acceptor note on the sales ticket any special terms and conditions regarding its refund policy.
5. The card acceptor mails a letter of confirmation, a copy of the sales ticket, including the reservation confirmation number, and information concerning its cancellation and refund policy to the cardholder at the address previously provided.
6. The card acceptor deposits the sales ticket for the advance deposit in the usual manner. There are no special deposit requirements imposed on the card acceptor outlet.

7. If a cardholder cancels his or her reservation in accordance with the agreed upon procedures, the hotel, motel, or resort is obligated to cancel the reservation and issue a credit to the cardholder.

    a. The card acceptor prepares a credit slip in the usual manner for the amount of the previously-submitted advance deposit, writing the words "deposit cancellation" in place of the cardholder's signature on the credit slip.

    b. The card acceptor prepares a notice of cancellation issuing a cancellation number to the cardholder.

    c. The card acceptor mails a copy of the credit slip and notice of cancellation to the cardholder.

    d. The card acceptor records the cancellation number on the slip and deposits the credit slip in the usual manner. There are no special deposit requirements imposed on the card acceptor outlet.

8. If the transaction results in a dispute, and if the account number used to make the deposit is unidentifiable as to a specific issuer or was fictitious, the bearer of the liability will be the acquirer. Where the transaction is identifiable to a specific issuer but is not identifiable to a specific account number within that institution, the bearer of the liability will be the acquirer.

4 *Excerpts from* GCMS Reference Manual *(published May 2005)*

This chapter contains excerpts of the GCMS Reference Manual *published May 2005. This* Merchant Rules Manual *contains only information applicable to merchants; therefore, some sections provided in the* GCMS Reference Manual *may have been omitted herein.*

Processing Unique Transactions

This subsection describes the following information specific to processing unique transactions:

- Acquirer and card acceptor obligations and rules
- Card acceptor business codes (MCCs)
- Indemnification guidelines

Completing the Unique Transaction at a POI Terminal

At card acceptor locations processing unique transactions via a POI terminal, if the card embossed account number does not exactly match the account number printed on the terminal receipt or displayed on the terminal, the card acceptor must follow the actions detailed under "Completing the Cash Disbursement Transaction at a POI Terminal," earlier in this chapter.

Acquirers must incorporate the following requirement into card acceptor agreements with gambling merchants and ensure compliance therewith:

A card acceptor must not credit winnings, unspent chips, or other value usable for gambling to a MasterCard cardholder account.

Processing Procedures for Non–Face-to-Face Unique Transactions

Acquirers must properly identify all unique transactions in all authorization and clearing messages. In addition, acquirers must ensure that electronic commerce transactions are properly identified in the authorization and clearing messages as defined in the *IPM Clearing Formats* manual and in the *Customer Interface Specification* manual.

Acquirers must incorporate the following requirements into all card acceptor agreements with Internet casino card acceptors:

- Internet casino card acceptors must request that cardholders identify the state or foreign country where they are physically located at the time of the transaction. They must record the response and retain it, along with the cardholder's account number, the transaction amount, and the date. Internet casino card acceptors must retain this information for a minimum of one year from the transaction date and provide it to the acquirer on request.

- As a condition of having a card acceptor's account with a MasterCard acquirer, Internet casino card acceptors must post a notice on their Web sites (in a position such that the notice will be displayed before requesting a MasterCard account number, such as a click-through notice) stating that assertions have been made that Internet gambling may not be lawful in some jurisdictions, including California, and suggesting that the cardholder check whether Internet gambling is lawful under applicable law.
- Internet casino card acceptors must not sell chips or other value that can be used, directly or indirectly, to gamble other than at a merchant that sells such chips or other value.
- Internet casino card acceptors must not credit winnings or unspent chips or other value usable for gambling to a MasterCard cardholder account.

Applicability of Standards

Transactions covered by this chapter are subject to MasterCard Standards governing retail sales transactions except as otherwise provided here and under "Indemnification."

- The floor limit for all unique transactions shall be zero.
- With the exception of truck stop transactions and of card-read transactions where a non-signature CVM is used, if a unique transaction is processed in a face-to-face environment, the cardholder must present a personal identification of the cardholder identical to that required for a cash disbursement as follows:

  The identification must be an official government document that has not expired and bears the customer's signature (for example, a passport, identification document, or driver's license).

  Acquirers should ensure that their card acceptors shall, to the extent allowed by applicable law, record on the face of the TID:

  – A description of the identification.
  – Any serial number, expiration date, and jurisdiction of issue.
  – The name of the customer (if not the same as the embossed name).
  – The address of the customer.

Except for card-read transactions where a non-signature CVM is used, to ensure that the cardholder's signature compares favorably in accordance with section 5.9 of the *Chargeback Guide,* the signature on the MasterCard card must be compared to:

– The cardholder's signature on the identification presented, and

– The cardholder's signature on the TID.

If the identification has a photograph of the cardholder, the card acceptor must check that the person presenting the card appears to be the same person.

- Authorization requests and clearing messages shall identify the transactions as unique.

Processing Payment Transactions

The following subsections describe acquirer and card acceptor obligations and rules, card acceptor business codes (MCCs), and indemnification guidelines specific to processing Payment Transactions.

Acquirer Obligations

Each acquirer is responsible for using the proper transaction type code in the transmission of information on transactions generated by its card acceptors.

The acquirer must submit Payment Transactions with a Processing Code (DE 3, subfield 1) = 28 and use the specified four-digit MCC as specifically defined in this manual under "Payment Transactions for Card Acceptor Activities—Four-Digit Card Acceptor Business Codes." However, acquirers participating in a local business service arrangement may submit Payment Transactions with a Processing Code (DE 3, subfield 1) = 28 and any MCC defined within their specific agreement.

In addition, first presentment messages should include the descriptor "C01" in the Program Registration ID (PDS 0043). Acquirers participating in a local business service arrangement may also use the other values in PDS 0043 such as C02 for Rebates and C03 for Load Value.

The acquirer also should provide either the customer service phone number or the URL address.

IF the acquirer provides the…	THEN the acquirer must place this data in…
Customer service phone number	Subfield 1 of Card Acceptor Inquiry Information (PDS 0170).
URL address	Card Acceptor URL (PDS 0175).

The message originator may submit a Payment Transaction Detail addendum with a first presentment payment transaction. This addendum provides the issuer and cardholder with enhanced data about the card acceptor, the recipient of funds, and other transaction details.

MasterCard, at its discretion, may monitor member and card acceptor compliance with the provisions set forth in this chapter under "Indemnification."

Member Registration Procedures for Registered Payment Transaction Providers

A Payment Transaction is a transfer of funds to a MasterCard account via the MasterCard interchange system. A Payment Transaction is not a credit that reverses a previous MasterCard purchase. A Payment Transaction may only be effected:

- By a member pursuant to a Business Service Arrangement (BSA) agreement; or
- Pursuant to a MasterCard program; or
- By a member or non-member as a registered Payment Transaction Provider (PTP).

When determining whether to register a member or merchant to use the Payment Transaction as a PTP, MasterCard considers various factors, including but not limited to, the following:

- The member or merchant's financial condition
- The adequacy of Payment Transaction disclosures to the cardholder (for example, disclosure of transactional limitations, such as per-day maximum Payment Transaction limits that apply across all payment methods)
- Cardholder procedures for inquiries and disputes
- Risk management procedures

Compliance with MasterCard Standards

MasterCard retains sole discretion of a registration decision, which is final and not subject to appeal. MasterCard also reserves the right to audit or to monitor any Payment Transaction or PTP and approve, disapprove, or rescind approval of a Payment Transaction program, PTP registration, or both, at any time.

Payment Transactions for Card Acceptor Activities—Four-Digit Card Acceptor Business Codes

Members may not submit Payment Transactions as unique (with a processing code [DE 3, subfield 1] value of 18). Instead, acquirers must submit Payment Transactions with the Payment Transaction processing code (DE 3, subfield 1 value of 28). Members must process Payment Transactions using the specific card acceptor business codes (MCCs) assigned, unless they participate in a local business service arrangement.

Payment Transaction Provider—Member Financial Institution—Payment Transaction (MCC 6532).

Payment Transaction Provider—Merchant—Payment Transaction (MCC 6533).

Acquirers participating in a local business service arrangement may use different MCCs.

Cardholder-Activated Terminal Requirements

Cardholder-activated terminals (CATs) are usually unattended terminals that accept bankcards, debit, charge, and proprietary cards. These terminals are frequently installed at rail ticketing stations, petrol stations, toll roads, parking garages, and other card acceptor locations.

The MasterCard CATs program includes four types of cardholder-activated terminals:

- Automated Dispensing Machines/Level 1
- Self-Service Terminals/Level 2
- Limited Amount Terminals/Level 3
- In-flight Commerce (IFC) Terminals/Level 4

Cardholder-activated terminal requirements specify the maximum dollar amount of transactions permitted as well as authorization, clearing, chargeback, and addendum record requirements and related transaction liability for each cardholder-activated terminal type.

Because these terminals are usually unattended, the traditional point-of-interaction (POI) acceptance procedures do not apply, such as the clerk's examination of the card to detect abnormalities in the MasterCard logo, hologram, embossed account number, or embossed security features and the comparison of the cardholder signature to the signature on the transaction receipt.

MasterCard also offers a means of identifying electronic commerce transactions using a value of CT6 in Terminal Type (PDS 0023) within First Presentment/1240, Chargeback/1442, Second Presentment/1240, and Arbitration Chargeback/1442 messages. There are currently no registration requirements established for these types of transactions, however, MasterCard requires acquirers to identify electronic commerce transactions using a value of CT6 in Terminal Type (PDS 0023).

In addition, members can use a CAT level indicator 7 (a value of CT7 in Terminal Type [PDS 0023]) to identify transponder transactions. Acquirers may optionally provide a value of CT7 in Terminal Type (PDS 0023) in First Presentment/1240, First Chargeback/1442, Second Presentment/1240, and Arbitration Chargeback/1442 messages.

General Requirements

The following six general acceptance requirements apply to cardholder-activated terminals:

1. All non–face-to-face transactions initiated by the cardholder where the card number is either captured as a result of reading the card electronically or by using an electronic device (such as a transponder, PC, or mobile phone) must include the proper cardholder-activated terminal (CAT) level indicator in both the authorization message and clearing records. Depending on the CAT level indicator, other specific data is required for authorization and clearing.

   (Refer to chapter 11 of the *Customer Interface Specification* manual and to the following section in this manual).

   a. The Authorization Request/0100 message must include a valid card acceptor category code, POS country code, POS postal code, and CAT level indicator (Level 1, 2, 3, 4, 6, or 7).

   b. Messages used at the CAT must communicate to the cardholder, at a minimum, the following:

      (i) Invalid transaction

      (ii) Unable to route

(iii) Invalid PIN—re-enter (Level 1 only)

(iv) Capture card (subject to the terminal's ability to retain cards)

c. The card acceptor identification number and the CAT level indicator must be present in the First Presentment/1240, First Chargeback/1442, Second Presentment/1240, and Arbitration Chargeback/1442 messages. (Refer to the *IPM Clearing Formats* manual for more information.)

2. The acquirer must ensure that the description of goods or services on the CAT TID is clearly recognizable to the cardholder.

3. The acquirer is responsible for providing requested transaction information documents in accordance with chapter 6 of the *Chargeback Guide*.

4. No cardholder-activated terminal may accept a MasterCard card for the purchase of scrip.

5. MasterCard reserves the right to modify the requirements and the procedures associated with cardholder-activated terminals, or to decline or withdraw processing permission, at its sole discretion.

6. Acquirers must ensure that transaction receipts provided to cardholders reflect only the last four digits of the primary account number, and that all preceding digits are truncated. MasterCard also requires that truncated digits be replaced with fill characters such as "X," "*," or "#" and not with blank spaces or numeric characters.

Terminal Level Requirements

The following acceptance requirements apply to the specific cardholder-activated terminals levels indicated.

Automated Dispensing Machines (ADMs)/Level 1

1. The Automated Dispensing Machine (ADM) must accept a personal identification number (PIN) as a substitute for signature, and ensure that all requirements are met in accordance with the MasterCard published specifications.

   a. The PIN requirement is contingent upon PIN being adopted as a standard within a country as well as issuers providing the required PIN. If PIN is not adopted as a standard within a country or supported in accordance with the MasterCard processing requirements for PIN-based transactions, this level of service is not available.

b. The PIN authorization must be made via a secured transmission, in accordance with the MasterCard published specifications.

c. ADM terminals must be able to support numeric, alpha, or alphanumeric PINs with a minimum length of four digits and a maximum length of six digits.

2. The acquirer may decline a transaction after four attempts and four consecutive negative responses of "invalid PIN" or "invalid transaction" from the MasterCard network. Optionally, the acquirer may allow more than four consecutive PIN entry attempts that each received a negative response at an ADM.

3. All transactions regardless of amount must be authorized on a zero floor limit basis with full, unaltered card read data transmitted. All acquirers of ADMs must have received one-time CVC certification from MasterCard.

4. Card retention at an ADM is not required, however, if the terminal capability is available, the card acceptor may do so only at the issuer's specific direction.

   a. The retained card must be logged and secured under appropriate audit controls, in accordance with chapter 1 of the *Security Rules and Procedures* manual.

   b. The retained card must promptly be rendered useless and then returned to the acquirer in accordance with chapter 1 of *Security Rules and Procedures* manual.

5. "No Cardholder Authorization" (reason code 4837) chargeback rights for this reason code are not available to issuers for transactions processed at ADMs where a PIN and full, unaltered card read data is transmitted because PIN is a valid proxy for the cardholder's signature.

6. The acquirer shall indemnify and hold harmless MasterCard and any and all issuers regarding any losses or damages associated with ADM terminals and PIN transmission arising from or related to any failure to adhere to the then current PIN security requirements or otherwise with MasterCard rules then in effect.

7. An ADM that is also a hybrid terminal may perform fallback procedures unless it is prohibited by a region. Members use fallback procedures when a smart card is present at a hybrid terminal and the card acceptor processes the transaction by using the magnetic stripe or by manually entering the PAN because the card acceptor cannot process the transaction using smart card technology.

Self-Service Terminal/Level 2

1. Self-Service Terminals do not process PIN. They include (but are not limited to) automated fuel dispensers identified with MCC 5542.

2. All Self-Service Terminal (SST) devices must comply with the following requirements:

   a. Zero floor limit for authorization purposes.

   b. Acquirer must read and transmit full, unaltered card read data.

3. The Authorization System will send all transactions identified as Self-Service Terminals in the Authorization Request/0100 message to the issuer's host, regardless of Limit-1 parameters. See chapter 2 of the *Authorization System Manual* for information about Limit-1 processing.

4. The maximum transaction amount is USD 100 or its equivalent.

5. Chargebacks processed for reason code 4837, "No Cardholder Authorization," for Self-Service Terminal transactions will be allowed only if the issuer certifies that the account number used in the transaction is fraudulent, as documented in a letter written by the cardholder to the card issuer.

   In addition, the issuer must block the account number(s) on the issuer's host until card expiration on or before the Central Site processing date of chargeback reason code 4837, "No Cardholder Authorization." The issuer also must list the cardholder account number on the MasterCard Account File with a "capture card" response until card expiration. Issuers in the Europe region (region D) also must list such accounts on the European Stop List (ESL).

   Counterfeit transactions occurring at Self-Service Terminals for which the acquirer has transmitted the full magnetic stripe data in the authorization request message and for which an authorization was obtained are ineligible for chargeback reason code 4837, "No Cardholder Authorization."

6. A U.S. region card acceptor acquiring automated fuel dispenser transactions at Self-Service Terminals/Level 2 may forward an Authorization Request/0100 message for USD 1 if properly identified by MCC 5542 (automated fuel dispenser) and CAT level indicator 2. If authorization is obtained, the acquirer is protected from authorization related chargebacks "requested/required authorization not obtained" (reason code 4808), or "exceeds floor limit—not authorized and fraudulent transaction" (reason code 4847) for transactions less than or equal to USD 75. The acquirer protection is limited to USD 75 for transactions that exceed USD 75, and issuers may charge back only the difference between the transaction amount and the implied USD 75 limit.

7. A Self-Service Terminal that also is a hybrid terminal may perform fallback procedures from chip to magnetic stripe unless it is prohibited by a region.

Limited Amount Terminals/Level 3

1. A Limited Amount Terminal must check the account number against the Electronic Warning Bulletin file if the terminal has such a capacity.

2. Maximum transaction amount is USD 40 or its equivalent.

3. Chargeback rights for reason code 4837, "No Cardholder Authorization," are not available to issuers for properly identified CAT/Level 3 transactions. Chargeback rights for "requested/required authorization not obtained" (reason code 4808), or "exceeds floor limit—not authorized and fraudulent transaction" (reason code 4847) are available if the maximum transaction amount of USD 40 or its equivalent has been exceeded.

4. A Limited Amount Terminal that also is a hybrid terminal is **prohibited** from performing fallback procedures from chip to magnetic stripe.

In-flight Commerce Terminals/Level 4

1. Acquirer/Service Provider Requirements and Transaction Identification Specifications

   a. Acquirers must ensure timely delivery and installation of the IFC Blocked Gaming File to gaming service providers. IFC Blocked Gaming File access is required before every gaming transaction.

   b. The acquirer must identify in-flight commerce services or merchandise with the most appropriate card acceptor category code (MCC) in the authorization message and card acceptor business code (MCC) in First Presentment/1240 messages. If an airline also acts as the service provider, the acquirer may not use an airline MCC but must assign the proper MCC for each type of IFC transaction. The following list of IFC transaction types must be identified with the designated MCC.

IFC Transaction Type	MCC
Catalog card acceptor	5964
Duty-free store	5309
Gaming	7995
Miscellaneous services	7299
Video game	7994

   c. Transactions must be consolidated by MCC, per flight, for each MasterCard cardholder account. "Flight" is defined as one or more segments of a continuous air flight with the same flight number.

   d. The acquirer must identify the transaction with the most appropriate transaction category code (TCC) in the authorization request message.

IF the IFC transaction is for…	THEN the acquirer must use TCC…
Gaming	U for Unique Transaction.
Anything other than gaming	R for Retail Purchase

   e. The Card Acceptor Name/Location (DE 43) must include the service provider's name and flight identification. The flight identification must be a recognizable identification of the airline (not necessarily the airline alphabetic International Air Transport Association [IATA] indicator).

f. The city field description should contain the following:

For…	The city field description…
Mailed purchases and gaming transactions	Must include the service provider's customer service telephone number. It is not required to be a toll-free number.
All IFC transactions other than mailed purchases and gaming	Optionally may be a customer service telephone number.

g. For all IFC transactions except IFC mailed purchase transactions, the transaction date is defined as the date that the flight departs from the originating city. The transaction date for mailed purchases is defined as the shipment date unless otherwise disclosed to the cardholder.

h. The acquirer must ensure that the service provider provides full disclosure to the cardholder via the video monitor screen prior to the initiation of any IFC transactions, as detailed below. The screen must prompt the cardholder to acknowledge these disclosure terms before initiating transaction(s). Disclosure must include the following:

(i) Full identification of the service provider and provision for recourse in terms of cardholder complaints or questions;

(ii) Notification that transactions will be billed upon the issuer's approval of the authorization request;

(iii) For mailed purchases only, any additional shipping or handling charges;

(iv) Policy on refunds or returns; and

(v) Provision for a paper receipt.

For IFC gaming transactions, service providers must additionally disclose the following:

(i) Maximum winnings (USD 3,500) and maximum losses (USD 350);

(ii) Notification that total net transaction amount (whether a net win or loss) will be applied against the cardholder's account;

(iii) Notification that cardholder must be at least 18 years of age to play; and

(iv) Notification that some MasterCard card issuers may not allow gaming.

i. The acquirer must ensure that the service provider is capable of providing an itemized receipt to the cardholder for all IFC transactions. The acquirer must ensure that, at the cardholder's option, the service provider can effect this offer in one of three ways:

(i) Printing a receipt at the passenger's seat,

(ii) Printing a receipt from a centralized printer on the plane, or

(iii) Mailing a receipt to the cardholder.

The mailed receipt offer is to be made available via the video monitor and must require the cardholder to input his or her name and address. For IFC gaming transactions the service provider must provide a receipt to the cardholder by methods (1) or (2), described above.

The receipt must contain the following elements:

(i) Identification of the passenger's flight, seat number, and date of departure;

(ii) Itemized transaction detail;

(iii) Gaming transaction specified as a net win or net loss; and

(iv) The cardholder's account number truncated on the receipt. Acquirers must ensure that transaction receipts provided to cardholders reflect a minimum of four and a maximum of 12 digits of the cardholder account number. The remaining digits are to be truncated, or rendered indeterminable. In all cases, at least four digits must be truncated. MasterCard recommends that the receipt reflect only the last four digits of the primary account number, and that all preceding digits are truncated. MasterCard also recommends that members replace truncated digits with fill characters such as "X", "*", or "#" and not with blank spaces or numeric characters.

j. For IFC terminals, the assurance and demonstration of security of the transmission of authorization and clearing data between the on-board client server and the acquirer and the physical controls over hardware and operating software. Encryption of transmitted data is advised.

2. Transaction Requirements

   a. No maximum transaction amount applies to any IFC transaction, with the exception of IFC gaming transactions.

   b. An IFC terminal that also is a hybrid terminal is **prohibited** from performing fallback procedures from chip to magnetic stripe.

3. Additional Requirements for IFC Gaming Transactions

   a. Net gaming losses cannot exceed USD 350 per flight per MasterCard cardholder account. Net payouts to cardholders for gaming wins cannot exceed USD 3,500 per flight per MasterCard cardholder account. This must be monitored throughout the flight by the service provider to ensure compliance.

   b. A gaming win transaction will result in posting of net winnings (credit) to the cardholder's account. Under no circumstance may winnings be paid in cash or other form of payment.

   c. Before participating in IFC gaming activity, the acquirer must undertake all reasonable and necessary steps to assure itself and, if requested, MasterCard International that such IFC gaming activity will be effected in full compliance with all applicable laws and regulations. By participating in IFC gaming activity the member agrees to indemnify, defend, and hold MasterCard harmless with respect to any claim, damage, loss, fine, penalty, injury, or cause of action arising or resulting from or attributable to the member's IFC gaming activity.

4. Cardholder Account Number Verification—In-flight Verification Prior to Transaction Initiation

   a. The acquirer must ensure that the service provider conducts a Mod-10 check digit routine to verify card authenticity.

   b. The acquirer must ensure that the service provider confirms that the card account number is within a valid MasterCard BIN range and must begin with 51, 52, 53, 54, or 55.

   c. For IFC gaming transactions, the acquirer must ensure that the MasterCard cardholder's account number is checked against the IFC Blocked Gaming File. Cardholders whose account numbers are listed on the IFC Blocked Gaming File must be prohibited from initiating any IFC gaming transaction.

5. Authorization Requirements for all IFC Transactions

   a. The Authorization Request/0100 message must include the cardholder-activated terminal level 4 indicator.

   b. The acquirer must read and transmit full, unaltered card read data. An IFC authorization request may not contain a key-entered account number or expiration date.

   c. Transactions are either authorized air-to-ground during the transaction or authorized in a delayed batch. All are authorized on a zero floor limit basis.

   d. The acquirer must convert all "refer to card issuer" and "capture card" messages received from issuers to "declines."

6. Additional Authorization Requirements for IFC Gaming Transactions

   All IFC gaming losses authorized post-flight must be submitted for authorization for the net amount. All gaming transactions authorized during the flight will be for the full wager amount (USD 350 or a lower amount predetermined by the airline and gaming service provider). No gaming wins will be submitted for authorization.

7. Clearing Requirements for all IFC Transactions

   a. An acquirer is not permitted to submit declined transactions (including those defined in 5.d. above) into clearing.

   b. No surcharges or service fees may be assessed on any IFC transaction, including IFC gaming transactions.

8. Additional Clearing Requirements for IFC Gaming Transactions

   a. IFC gaming transactions submitted for clearing must be for the net amount that is won or lost.

   b. IFC gaming win transactions will be submitted as a credit transaction (Processing Code [DE 3, subfield 1] = 20). Interchange will be paid to issuers by acquirers on gaming win transactions.

   c. An acquirer may resubmit a gaming transaction for a different amount within the specified transaction limits if it was previously rejected for exceeding the specified transaction limits—USD 3,500 for wins and USD 350 for losses.

9. Effective Date of the IFC Blocked Gaming File

   Updates to the IFC Blocked Gaming File will be effective on the first and the 15th day of each month. MasterCard must receive account ranges or BINs that issuers choose to list on the next effective updated IFC Blocked Gaming File at least two weeks before the effective date.

5 *Excerpts from* Security Rules and Procedures *(published July 2005)*

This chapter contains excerpts of the Security Rules and Procedures *manual published July 2005. This* Merchant Rules Manual *contains only information applicable to merchants; therefore, some numbered sections provided in the* Security Rules and Procedures *manual may have been omitted herein.*

3.7 Transaction Information Documents (TIDs)

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

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

If the merchant uses a manual imprinter, the TID produced is called a formset or slip. For MasterCard formset specifications, refer to Appendix D.

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.

3.7.1 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:
  - 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 identifies 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 member that distributed the slip to the merchant.

3.7.2 Terminal Receipt Contents

A terminal or other device at a point of interaction must not display magnetic stripe track data other than card account number, expiration date, and cardholder name.

Each copy of a 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
- Transaction amount in the original transaction currency
- Adequate space for the customer's signature (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 smart card transactions.
- Merchant's signature on credit receipts only

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

3.7.3 Primary Account Number Truncation

MasterCard requires ATM acquirers to truncate, or render indeterminable on printed ATM receipts, a minimum of four digits of the PAN. MasterCard also requires PAN truncation for all receipts generated at Cardholder-Activated Terminals (CATs). PAN truncation is permitted for receipts generated at all other points of interaction.

MasterCard strongly recommends that all cardholder receipts generated by POI terminals, whether attended or unattended, reflect only the last four (4) digits of the PAN, replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as "X," "*," or "#."

Effective 1 April 2005, the cardholder receipt generated by newly installed, replaced, or relocated POI terminals, whether attended or unattended, must reflect only the last four (4) digits of the PAN. All preceding digits must be replaced with fill characters that are neither blank spaces nor numeric characters, such as "X," "*," or "#."

3.7.3.1 Truncation Considerations

Truncating a greater number of digits, when compared to the total number of digits in the PAN, increases the effectiveness of the effort. However, it also increases the confusion and difficulty that cardholders may have reconciling their ATM terminal receipts to their periodic statements, therefore a satisfactory balance must be reached.

1. Truncation of the routing BIN alone, while helpful, may not prevent duplication of the PAN. It is possible to observe the card in use in order to obtain issuer identification.
2. Truncating the check digit and several other digits does not improve PAN security. Absent the check digit, calculation of several missing digits within the PAN, especially if the routing BIN also is truncated, is substantially more complicated and time consuming.
3. Truncating a small number of digits, when compared to the total number of digits in the PAN, reduces the effectiveness of the effort. It is possible to reconstruct a few missing digits by using a trial-and-error approach.
4. Truncating a greater number of digits, when compared to the total number of digits in the PAN, increases the effectiveness of the effort.

3.7.4 Electronic Signature Capture Technology (ESCT)

An acquirer 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 card acceptor 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 members to ensure compliance with these sections and may prohibit use of ESCT if it identifies inadequate controls.

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 Automated Dispensing Machines (ADMs)/Level 1 Cardholder-Activated Terminals. A PIN also may be used at certain other point of interaction (POI) terminals.

All members must comply with the security requirements for PIN and key management as specified in the following International Organization for Standardization (ISO) documents:

- ISO 9564-1, Personal Identification Number management and security, Part 1: "Basic principles and requirements for online PIN handling in ATM and POS systems"
- ISO 9564-2, Personal Identification Number management and security, Part 2: "Approved algorithms for PIN encipherment"

Each member also must comply with the security requirements for PIN and key management set forth in the following documents published by MasterCard International:

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

For additional information about PIN key management and related services, refer to the manuals listed in Figure 4.1, which are available through the MasterCard OnLine® Member Publications tool.

Figure 4.1—PIN Key Management References

For transaction authorization request messages routed through…	Refer to…
Banknet	*Authorization System Manual*
MasterCard Debit Switch (MDS)	*MDS Online Specifications*
EPS-Net	*EPSS Security Platform (ESP) Document Set*
Regional Service Center	*Network Security Platform (NSP) Document Set*
MasterCard Key Management Centre via the On-Behalf Key Management (OBKM) Interface	*On-Behalf Key Management (OBKM) Document Set*

4.3 PIN Usage Standards

Issuers must comply with the following PIN Usage Standards established by MasterCard.

4.3.3 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 Automated Dispensing Machines (ADMs)/Level 1 Cardholder-Activated Terminals (CATs).

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.

MasterCard 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 4.6 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 rules. All other POI transactions containing PIN data will be declined in Stand-In processing.

4.4 PIN-based Terminal Standards

All PIN-based terminals must have the capability to:

- Read and transmit unaltered, full track data (track 1 or 2)
- Display messages on the terminal indicating the different steps to be taken by the merchant during the transaction
- Mandate that the standard message language be English, and offer optional local language
- Have an online connection to the acquirer for the authorization of all PIN-based magnetic stripe transactions
- Ensure to the cardholder the privacy of PIN entry
- Prevent additional transactions from being entered into the system when the transaction is being processed
- Maintain a terminal transaction log that does not include the cardholder's PIN information or derived PIN data
- Provide a transaction information document (TID) either automatically or upon customer request. The TID must include the transaction time, trace number, terminal number, and other MasterCard terminal receipt content requirements.

4.4.1 Security Provisions for EMV Hybrid Terminals Supporting Offline PIN

Hybrid terminals support both magnetic stripe and integrated circuit cards (ICCs).

The following Standards address all Europay-MasterCard-Visa (EMV) hybrid terminals supporting offline PIN transactions:

- All new terminals that support offline PIN transactions must support both clear text and enciphered offline PIN options.
- Retrofitted terminals that support offline PIN transactions should support both clear text and enciphered offline PIN options, if possible.

Hybrid terminals must support online dynamic CAM for all chip-read transactions.

Note **All terminals that support offline PIN transactions must support both clear text and enciphered offline PIN options by 1 January 2005.**

4.5 PIN Encryption Standards

Whenever the PIN is electronically transmitted outside a secure cryptographic device, it must be cryptographically protected using the approved algorithm(s) for PIN encipherment listed in ISO 9564-2. MasterCard must approve the use of other algorithms.

For online PIN transmission, the encrypted PIN block format must comply with ISO 9564-1 format 0, format 1, or format 3. For offline PIN verification by a smart card (either plain text or enciphered), ISO 9564-1 PIN block format 2 must be used.

For ISO format 0 and 3, the cleartext PIN block and the Primary Account Number (PAN) must be Exclusive-OR'ed (XOR'ed) together and then Triple DES encrypted in Electronic Code Book (ECB) mode to form the 64-bit output cipherblock (the reversibly encrypted PIN block). ISO formats 1 and 2 are formed by the concatenation of the plaintext PIN field and the filler field.

MasterCard must approve the use of alternative equivalent formats. Any alternative format used in a local network must produce different enciphered PIN block results when the same PIN is associated with different accounts.

The PIN will remain encrypted until the issuer or the MDS receives it for verification.

Members must adhere to the following Standards for PIN encryption:

- Perform all PIN encryption, translation, and decryption for the network using hardware encryption by using physically secure devices (PSDs).
- Do not perform PIN encryption, translation, or decryption under Triple DES software routines.
- Acquirers must never log, even in encrypted form, issuers' PINs on journals, computer records, magnetic tapes and disks, or on any printed records resulting from interchange authorization of transaction records.
- Use the Triple DES algorithm to perform all encryption.

4.5.2 PIN Encryption at POI Terminals

At a minimum, all merchant POI terminals must use Single DES technology with a method of key management that derives one unique key per transaction. Preferred methods of key management include the use of Triple DES encryption and certain implementations of public key cryptography. Where public key cryptography is used, MasterCard will review and approve each implementation.

The POI terminal must encrypt the PIN in:

- a tamper-responsive or physically secure device (PSD); or
- a tamper-evident or minimum acceptable PIN entry device (PED).

Definition **Tamper-evident device—A type of tamper-resistant security module in which any attempt to penetrate the device will be obvious. Such a device can be used only for PIN encryption and key management schemes where penetration of the device will offer no information on previously entered PINs or secret keys. Also called a minimum acceptable PIN entry device.**

4.5.3 Triple DES Migration Schedule

All merchant POI terminals and ATMs are required to use Triple DES, minimum double key length (hereafter referred to as "Triple DES"), in accordance with the implementation schedule set out below:

- All newly installed merchant POI terminals and ATMs, including replacements, must be Triple DES capable.
- All member and processor host systems must support Triple DES.
- Effective 1 April 2005, all ATMs must be Triple DES compliant.
- Effective 1 April 2005, it is strongly recommended that all merchant POI terminals be Triple DES compliant and chip-capable.

MasterCard recognizes that members may elect to use other public key encryption methods between their merchant POI 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 that other method to be as secure as or more secure than Triple DES. **Approval is required before implementation can begin.** All transactions routed to the MasterCard system must be Triple DES compliant.

4.6 PIN Entry Device Standards

All cryptographic functions must be performed in a device that meets the requirements for a tamper-resistant security module (TRSM) in which all clear text keys and PINs are physically protected against disclosure and modification.

The following minimum security Standards regarding such PIN entry devices (PEDs) are consistent across all brands, services, and programs.

1. The PED must be designed and installed so that a third party is prevented from observing the PIN as it is being entered.
2. The PED must not display the PIN in plain text or disclose the PIN by audible feedback. Acoustic or visible signals to indicate data entry are recommended, provided they are neutral in tone and character and in no way reveal which letter or number has been pressed.
3. The PED must have a "clear" function to enable the cardholder to retract incorrect letter or number selections and an "enter" function to indicate completion of PIN entry.

4. The PED must be designed to protect the cardholder against deception about:
   - the normal sequence of transaction steps;
   - the fact that no PIN is required for signature-based POI transactions;
   - the information displayed or printed;
   - additional data requested;
   - the authorization response; and
   - the completion or cancellation of a transaction.

All PEDs must have unique keys. No two PEDs shall use the same encipherment keys for any PIN or key encryption purpose except by chance or random selection. Knowledge of the keys used in any given PED must not allow disclosure of the keys used in any other PED.

PED manufacturers must self-certify that their respective devices meet the minimum requirements identified in the PED Self-Assessment Questionnaire. This questionnaire sets the currently acceptable minimum implementations of physical security requirements as stated in ISO 9564.

If a member 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.

4.6.1 Tamper-Responsive Device Standards

To qualify as a tamper-responsive device, also known as a physically secure device, a PED must meet the following criteria:

1. Penetration of the device will cause immediate erasure of all PINs, cryptographic keys, and all useful residue of PINs and keys contained within it.
2. Key management techniques used in the PED includes one of the following:
   a. fixed transaction keys,
   b. master keys/transaction keys,
   c. a non-reversible transformed unique key per transaction, or
   d. a derived unique key per transaction.

The transmission medium (cable, wire) between the keyboard and the encipherment circuitry is highly protected physically and prohibits installation of tapping devices.

Each terminal supports a unique key.

4.6.2 Tamper-Evident Device Standards

To qualify as a tamper-evident device, also known as a minimum acceptable PIN entry device, a PED must meet the following criteria:

1. Any unauthorized attempt to penetrate it would be obvious.
2. The device is plastic or steel-encased, or otherwise impossible to penetrate without the proper equipment or expertise, or relocation to a specialized facility.
3. The PIN is enciphered within the device using an approved algorithm and PIN block format.
4. The device uses a unique key per transaction scheme (a key transformation or key derivation technique must be used to accomplish this).

5.1 Card Recovery and Return

The following subsections address member responsibilities associated with card retention and return, rewards for card capture, reporting of lost and stolen cards, and criminal and counterfeit investigations.

5.1.1 Point-of-Interaction (POI) Card Retention

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

1. The issuer advises the acquirer or merchant to recover the card in response to an authorization request.
2. 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 *MIM* under "Other Information," 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) embossed on the front of the card.
- The member ID imprinted in the Card Source Identification area on the back of the card.

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 Management department.

Note

The above method of identifying the issuer applies only to the return of a counterfeit card, not to determining the member responsible for the counterfeit losses associated with such cards. For more information, refer to chapter 6 of this manual.

5.1.1.3 Liability for Loss, Costs, and Damages

Neither MasterCard nor any member 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 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 members shall be liable for loss, costs, or other damages if a claim is made against them.

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

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

5.1.3 Payment of Rewards

The acquirer may pay the merchant or financial institution teller a reward for capturing a MasterCard card in accordance with local practice. The person capturing the card receives the reward. A reward payment is not required for capture of a Cirrus-branded or Maestro-branded card.

5.1.3.1 Reward Payment Standards

The acquirer must follow these Standards when paying a reward:

1. Pay no less than USD 50 to the merchant capturing a card listed on the Electronic Warning Bulletin file or in the *Warning Notice*.
2. Pay the merchant USD 100, **if** a merchant initiates an authorization call because of a suspicious transaction or captures a card not listed in the Electronic Warning Bulletin file or in the *Warning Notice*.
3. Pay a reward to a financial institution teller for the capture of another member's card if it is the acquirer's practice to pay its tellers rewards for picking up its own cards. The amount of the reward should be the same amount paid for the capture of the acquirer's own cards within the limits set forth in section 5.1.3.2.
4. Charge the issuer for reimbursement of the reward paid upon dispatching each card captured by either a merchant or a financial institution teller. The Fee Collection/1740 message with an IPM message reason code (data element 25) equal to 7601 will settle the reward.

5.1.3.2 Reward Amounts

The acquirer should follow these guidelines for determining reward amounts.

Figure 5.1—Amount Determinations

IF the capture…	THEN pay this amount…
Resulted from a "Merchant Suspicious" phone call	USD 100
Did not result from a "Merchant Suspicious" phone call	USD 50
Leads to the capture of additional cards	USD 50 for each card captured, with a maximum total of USD 250 for any one incident

The stipulation that the person capturing the recovered card receives the reward as stated in section 5.1.4 does not prevent members from making mutually acceptable agreements between themselves regarding rewards.

The recovering member may collect an administrative fee of USD 15 for expenses incurred in processing the captured card. The capturing member may add this fee to the amount of the reward reimbursement or collect the fee independently, using the Fee Collection/1740 message.

5.1.3.2 Reimbursement of Rewards

The following specifications apply to reward reimbursement:

1. Upon dispatching the card to the issuer, the acquirer will obtain reimbursement for the reward paid and the USD 15 fee by processing the Fee Collection/1740 message.
2. If a member returns a card to an issuer and a reward is not paid, the recovering member may, at its discretion, collect a USD 15 fee by processing a Fee Collection/1740 message record.
3. Upon receipt of the Interchange Card Recovery Form (ICA-6), the issuer should match it to the Fee Collection/1740 message record based on the acquirer member ID, account number, and recovery date comparisons.
4. If an exempt member has an electronic reward payment processed, clearing receives the record by an information slip. The transaction is part of the Net Settlement System for settlement purposes. (Refer to the *Quick Reference Booklet* for a listing of exempt members.)

5.1.3.3 Reward Payment Chargebacks

A reward reimbursement draft may be charged back only when the incorrect member is charged. The senior vice president of the Security and Risk Management department will resolve any dispute concerning reward reimbursement.

5.1.4 Reporting Fraudulent Use of Cards

Reporting fraudulent use of MasterCard cards must be in accordance with MasterCard fraud reporting categories, as may be established from time to time. (Refer to chapter 12, "System to Avoid Fraud Effectively (SAFE)," for more information.)

Members should use SAFE to create FDN Records.

All MasterCard members must report accurately and completely the fraudulent use of MasterCard cards to SAFE at least once a month and within 60 days from the date of the transaction, or 30 days from the date of cardholder notification. If there are no fraudulent transactions to report during the month, members must submit a Fraud Negative Report (FDN) Record when transmitting their transactions to SAFE or use the **Report No Fraud** feature of SAFE OnLine.

5.1.4.1 Reporting by the Issuer

MasterCard issuers must submit all fraudulent transactions on its MasterCard accounts to SAFE on a monthly basis. For the benefit of all members, MasterCard analyzes the data and produces statistics relating to the fraudulent use of MasterCard accounts and all chargebacks that originate from transactions using accounts with a fraud status.

An issuer must report fraudulent transactions even if it recovered losses through chargebacks, compliance cases, restitution, insurance, or any other means.

5.1.4.2 Reporting by the Acquirer

An acquirer receiving a transaction that cannot be identified by a MasterCard BIN or member ID is liable for that transaction. If it is determined that the transaction is a fraudulent or counterfeit MasterCard transaction, the acquirer must notify, in writing, the Security and Risk Management Department of such an occurrence. This notification must include all mandatory information as described in the *Security Systems Specifications* manual.

5.1.5 Reporting Lost and Stolen Cards

A member or its affiliate, or a third-party processor acting as its authorized agent that receives a lost or stolen card report must promptly notify the issuer of the report. The member should send the notice via phone and direct it to the issuer's security contact identified in the *Member Information Manual (MIM)*.

The notice must include all relevant available information, such as:

- Member ID of the institution sending the notice
- Issuer's name
- Cardholder account number
- Cardholder's name and address
- Phone number and an address where the cardholder can be reached

If the member cannot immediately reach the issuer by phone, the member must make another attempt at the first opportunity during the issuer's normal business hours. Issuers must accept all collect calls placed to report a lost or stolen card.

Note **The issuer will be responsible for the reasonable costs of transmitting the notice.**

For international notifications only, in lieu of a phone message, a telex or cable message is acceptable. The issuer is responsible for the reasonable costs of transmitting the notice and must accept collect calls. The notice should include the same information previously mentioned. In addition, the member making the report should follow the international notice with a written confirmation within three business days.

The member that receives and transmits the report may submit to the issuer an IPM Fee Collection/1740 message with message reason code 7600 to collect the USD 15 lost or stolen card report fee in addition to any transmission costs it may incur.

If the account number is unknown, the reporting member still may use the IPM Fee Collection/1740 message by zero-filling the Account Number field and by providing the cardholder's name and address, and the issuer name or service mark, in the Data Text field.

Note **Issuers may direct cardholders to the MasterCard Global Service Center Cardholder Emergency Hotline at 1-800-307-7309.**

5.1.5.1 MasterCard Receiving Reports

MasterCard will help its members by receiving lost or stolen card reports, and will (at each member's option) either take the report and promptly notify the issuer or, if the report is by phone, direct the call to the issuer (when such capability is available). MasterCard will, only at each issuer's request, promptly update the authorization negative file used for Stand-In processing.

MasterCard may charge the issuer USD 15 per report in addition to any transmission costs it may incur for receiving and transmitting the report.

6.2 Fraud Loss Control Program Standards

In order to be eligible for counterfeit loss reimbursement, a member must make a good-faith attempt to demonstrate to the satisfaction of MasterCard the existence and use of meaningful controls 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 Card Not Present (formerly MO/TO), voice, and e-commerce 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

6.2.2.1 Acquirer Authorization Monitoring Requirements

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

- Number of authorization requests above a threshold set by the acquirer for that merchant
- Ratio of non-card-read to card-read transactions that is above the threshold set by the acquirer for that merchant
- PAN key entry ratio that is above threshold set by the acquirer for that merchant
- Repeated authorization requests for the same amount or the same cardholder account
- Increased number of authorization requests
- "Out of pattern" fallback transaction volume.

6.2.2.2 Acquirer Merchant Deposit Monitoring Requirements

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

- Increases in merchant deposit volume
- Increase in a merchant's average ticket size and number of transactions per deposit
- Change in frequency of deposits
- Frequency of transactions on the same cardholder account, including credit transactions
- Unusual number of credits, or credit dollar volume, exceeding a level of sales dollar volume appropriate to the merchant category
- Large credit transaction amounts, significantly greater than the average ticket size for the merchant's sales
- Credits issued subsequent to the receipt of a chargeback with the same account number and followed by a second presentment
- Credits issued to an account number not used previously at the merchant location

90-day Rule

The acquirer must compare daily deposits against the average transaction count and amount for each merchant over a period of at least 90 days, to lessen the effect of normal variances in a merchant's business. For new merchants, the acquirer should compare the average transaction count and amount for other merchants within the same card acceptor business code (MCC) assigned to the merchant. In the event that suspicious credit or refund transaction activity is identified, if appropriate, the acquirer should consider the suspension of transactions pending further investigation.

150% Recommendation

To optimize the effectiveness of fraud analysis staff, merchants that appear in the monitoring reports should exceed the average by 150% or more. However, the amount over the average is at the acquirer's discretion.

6.2.2.3 Recommended Additional Acquirer Monitoring

MasterCard recommends that acquirers additionally monitor the following parameters.

- Fallback methods
- Credit transactions (such as refunds)

- Transactions conducted at high-risk merchants
- PAN key-entry transactions exceeding ratio
- Abnormal hours or seasons
- Inactive merchants
- Transactions with no approval code
- Transactions that were declined
- Authorization/clearing mismatch

7.1 Screening New Merchants

Before signing a merchant agreement, each member must verify that the merchant from which it intends to acquire MasterCard transactions is a valid business, as described in section 9.2 of the *Bylaws and Rules* manual. 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 member also should conduct a credit check of:

  a. The owner, if the merchant is a sole proprietor; or

  b. The partners, if the merchant is a partnership; or

  c. The principal shareholders, if the merchant is a corporation.

- Inspection of the premises and records to ensure 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 member must inspect at least one outlet from which it will acquire MasterCard transactions.

No member financial institution is exempt from participation in the MATCH system.

- Inquiry to the MasterCard Member Alert to Control (High-risk) Merchants (MATCH™) system. If a member chooses to enter into a merchant agreement with a merchant that is listed in the MATCH system, the member will be responsible for all fraudulent transactions.
- Investigation of the merchant's previous merchant agreements.

A member 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 member 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 member is in compliance with the screening requirements set forth in this chapter, MasterCard requires, at a minimum, the following information:

- A report from the 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 member's inquiry into the MATCH system, including a copy of the inquiry record
- A statement from the merchant about previous payment card 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 the agreement is terminated. MasterCard recommends that acquirers retain the following records as a best practice:

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

- 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 member correspondence with merchant
- All correspondence relating to issuer, cardholder, or law enforcement inquiries concerning the merchant or any associated Member Service Provider (MSP)
- Signed MSP contract, including the name of agents involved in the due diligence process
- Acquirer due diligence records concerning the MSP and its agents

7.1.4 Screening Limitations

Screening merchants, as required by the Standards, does not relieve a member 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 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.

7.2.1 Merchant Monitoring

An acquirer must monitor each of its merchant's MasterCard 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.

7.2.1.1 Additional Requirements for Certain Merchant Categories

Acquirers of key-entry telecom merchants, electronic commerce adult content (videotext) merchants, and merchants identified under the Excessive Chargeback Program must comply with the merchant registration and monitoring requirements of the Merchant Registration Program for each such merchant, as described in chapter 9.

7.2.1.1.1 Capital Requirements for Certain Merchant Categories

A member that acquires for a key-entry telecom merchant, an electronic commerce adult content (videotext) merchant, or a merchant identified under the Excessive Chargeback Program must, in any month, have Tier 1 capital or its equivalent, as defined by the member's regulatory agency, equal to three times the aggregate volume of the total of all payment card transaction volume processed for such merchants in that month. Refer to section 2.7 of the *Bylaws and Rules* manual and to the *Global Risk Management Policies and Procedures* booklet for more information.

7.2.2 Merchant Education

Once an acquiring relationship is established, an acquirer should institute a fraud prevention program, including an education process consisting of periodic visits to merchants, distribution of related educational literature, and participation in merchant seminars. Instructions to merchants must include card acceptance procedures, use of the Electronic Warning Bulletin file or *Warning Notice*, authorization procedures including Code 10 procedures, proper completion of Transaction Information Documents (TIDs) (including primary account number [PAN] truncation), timely presentment of the transaction to the acquirer, and proper handling pursuant to card capture requests. Members must thoroughly review with merchants the Standards against the presentment of fraudulent transactions. In addition, members 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.

8.1 Merchants Presenting Invalid 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 or the acquirer's own standards, or both.

An acquirer also must state its willingness to accept chargebacks for all fraudulent transactions that took place during the period when the merchant was in violation of section 9.14.1 of the *Bylaws and Rules* manual. If an acquirer fails to take such action, the acquirer becomes ineligible for possible reimbursement for fraud loss under the acquirer's counterfeit loss reimbursement program.

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 member's merchant file and records.

For more information on the acquirer's counterfeit loss reimbursement program, including eligibility requirements and application procedures, refer to section 6.3.5 of this manual.

8.1.2 Notifying MasterCard—Issuer Responsibilities

If an issuer becomes aware of any merchant in violation of section 9.14.1 of the *Bylaws and Rules manual*, through cardholder complaints or otherwise, the issuer immediately must notify Merchant Fraud Control staff.

8.1.3 MasterCard Audit

MasterCard, in its sole discretion, and either itself or by use of a third party, 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 MATCH system under MATCH reason code 00 (Questionable Merchant).

In the course of the audit, staff will develop allegations from any available sources, including, but not limited to, internal studies, analyses, member 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 section 9.14.1 of the *Bylaws and Rules* manual, MasterCard will send a letter to the Security Contact listed in the *Member Information Manual*. 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 the penalties associated with violations of section 9.14.1. Members 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 a MasterCard-initiated audit to determine whether an acquirer's merchant was in violation of section 9.14.1 of the *Bylaws and Rules* manual:

- A detailed statement of facts explaining whether, when, and how the member became aware of fraudulent activity or chargeback or customer service issues, the steps taken by the member to control the occurrence of fraud, and the circumstances surrounding the merchant's termination.

- 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.)
- All internal member 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 member verified during the due diligence procedure.
- If a Member Service Provider (MSP) of an acquirer facilitates the signing of a merchant, the MSP must include the due diligence documents. (If an MSP facilitates the signing of a merchant for an acquirer, the acquirer must distinguish between the due diligence conducted by its employees and its MSP's employees. This rule applies only to members in the U.S. region.)

  Additionally, if an acquirer's MSP assisted in the signing of the merchant, the member must provide all MSP due diligence documents regarding the representative that signed the merchant.
- Internal reports, where applicable, confirming inquiry by the member 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.
- Staff will establish an audit (review) period for which the member must provide the following supporting documentation:

  a. Authorization logs for the merchant.

  b. 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 violation period, as specified by MasterCard.

  c. 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. Members 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 that members provide additional information relevant to the audit. In the event that a member 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 section 9.14.1 of the *Bylaws and Rules* manual.

8.1.3.3 Notification to Members 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).

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 number of the *Global Security Bulletin* (for example, "*Global Security Bulletin* No. XX") must be included in the Data Record of IPM Data Element 72.

8.2 Merchant Audit Program

Effective 2 August 2005, MasterCard has replaced this program with the Global Merchant Audit Program (GMAP). Please proceed to section 8.4 of this manual for details about the GMAP.

8.3 Excessive Counterfeit Merchant Program

Effective 2 August 2005, MasterCard has replaced this program with the Global Merchant Audit Program (GMAP). Please proceed to section 8.4 of this manual for details about the GMAP.

8.4 Global Merchant Audit Program

The Global Merchant Audit Program (GMAP), using a rolling six months of data, identifies merchant locations that meet all of the following minimum criteria in any one calendar month:

- Three fraudulent transactions
- A cumulative total of at least USD 2,000 in fraudulent transactions
- A minimum fraud-to-sales ratio of 1%

The merchant locations identified under this program as meeting the minimum criteria are classified into the following three tiers based upon their fraud-to-sales ratio in any one month:

- *Tier 1*—A fraud-to-sales ratio minimum of 1% and not exceeding 3.99%
- *Tier 2*—A fraud-to-sales ratio minimum of 4% and not exceeding 6.99%
- *Tier 3*—A fraud-to-sales ratio of at least 7%

When a merchant is identified in different tiers during the rolling six-month period, GMAP will use the highest tier identification as the trigger month.

8.4.1 Repeated Identifications

If the merchant is identified in Tiers 1 or 2 more than one time in a 12-month period, GMAP automatically will escalate that merchant into the next higher tier.

GMAP will escalate merchants with more than one identification in Tier 1 to Tier 2, requiring the acquirer to provide additional training and fraud control mechanisms for the merchant.

GMAP will escalate merchants identified in Tier 1 and subsequently identified in Tier 2, or those identified more than one time in Tier 2, to Tier 3. Escalation of a merchant to Tier 3 will require an acquirer to decide whether to accept liability for fraud related chargebacks or to terminate the merchant agreement.

Escalation of a merchant into the next higher tier will be determined based upon the merchant's most recent prior identification.

Note **If a merchant has more than one location (or outlet), the program criteria apply to each location independently.**

8.4.2 Acquirer Responsibilities

MasterCard will notify and acquirer of the identification of a Tier 1, Tier 2, or Tier 3 merchant. MasterCard will ask the acquirer to provide information about the merchant. Upon receipt of the GMAP notice, the acquirer must act as indicated in Figure 8.1.

Failure of a member to respond to a MasterCard notification or take action as indicated in Figure 8.1, or failure of a member to provide the required documentation and supporting evidence as indicated in this chapter, may result in the merchant's being listed in a *Global Security Bulletin* with an applicable chargeback liability period.

If a merchant is terminated after the response due date, MasterCard reserves the right to list the merchant in a *Global Security Bulletin* with an applicable chargeback liability period.

As a result of the merchant's being listed on a *Global Security Bulletin*, the acquirer will be liable for chargebacks, as described in this chapter.

Figure 8.1—Acquirer Responsibilities by Global Merchant Audit Program Tier

	For a merchant location identified in Tier 1…	For a merchant location identified in Tier 2…	For a merchant location identified in Tier 3…
Action	MasterCard does not require the acquirer to respond formally to the GMAP notice; the Tier 1 notice is provided for information only.	The acquirer must conduct training on acceptance and fraud control procedures at the merchant location.	The acquirer either must terminate the merchant agreement or accept liability for chargebacks with Integrated Product Messages (IPM) reason code 4849—Questionable Merchant Activity for all reported fraudulent transactions (except Fraudulent Application and Account Takeover fraud) during the applicable chargeback period. MasterCard will determine the chargeback period to be a minimum of six months or a maximum of 12 months.
Response	MasterCard does not require the acquirer to respond formally to the GMAP notice; the Tier 1 notice is provided for information only.	The acquirer must provide a response, via MOST, for each merchant location identified in the Tier 2 criteria, within 30 calendar days of the date of the Tier 2 notice.	The acquirer must provide a response, via MOST, for each merchant location identified in the Tier 3 criteria, within 30 calendar days of the Tier 3 notice.
MasterCard Recommendation	MasterCard recommends that the acquirer implement or enhance a fraud control program.	MasterCard recommends that the acquirer implement or enhance a fraud control program.	MasterCard recommends that the acquirer, if it does not terminate the merchant, implement or enhance a fraud control program.

8.4.3 Chargeback Liability

Should an acquirer elect to accept chargeback responsibility, MasterCard will list the merchant name and location in a Global Security Bulletin with an applicable chargeback liability period.

An issuer then will have the right to charge back any MasterCard transaction timely reported to SAFE that occurred during the applicable period; provided that the issuer may not charge back for fraudulent transactions reported under the Fraudulent Application or Account Takeover (ATO) fraud types.

Once MasterCard lists a merchant in the *Global Security Bulletin*, the issuer chargeback rights will apply. The chargeback liability period will be for a minimum of six months and may, at staff discretion, be increased to a 12-month period for the reasons described in Figure 8.2.

Figure 8.2—Chargeback Liability Period and Determining Factors

Chargeback Period	Determining Factor
Six months	Less than USD 8,000 in cumulative fraud for three months following the month in which the identification criteria are met
12 months	More than USD 10,000 in fraud during the month in which the identification criteria are met **or** USD 8,000 or more in cumulative fraud for three months following the month in which the identification criteria are met

The applicable chargeback period shall commence on the first day of the month following the month in which MasterCard staff identifies the merchant in the GMAP.

Once MasterCard lists a merchant in a *Global Security Bulletin* with an applicable chargeback period, the issuer may not use the message reason code 4849—Questionable Merchant Activity, in any of the following situations:

- The transaction was not reported properly to SAFE within the applicable time frame specified in this manual.
- The transaction reported to SAFE was the result of a fraudulent application or account takeover.

- The merchant is SecureCode-enabled, the issuer provided the UCAF data for that transaction, 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 the transaction was processed at a chip compliant POI terminal, the intraregional chip liability shift program is in effect, the transaction was reported to SAFE as counterfeit fraud, the transaction was identified properly as an offline chip transaction in the clearing record, or the transaction was identified properly 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.

8.4.4 Exclusion from the Global Merchant Audit Program

All merchants processing MasterCard card transactions may be identified in the GMAP, with the exception of merchants that are excluded systematically or on a case-by-case basis following review.

8.4.4.1 Systematic Program Exclusions

The following systematic exclusions occur automatically, thus preventing such transactions from being accounted for in the identification of a merchant in the GMAP:

- *Debit Fraud*—This includes all fraud related to Cirrus (CIR), Maestro (MSI), and Eurocheque-Pictogram (ECH).
- *All Fraudulent Application and Account Takeover (ATO) fraud types*—This includes all fraud transactions reported to SAFE under the Fraudulent Application or Account Takeover fraud types.

8.4.5 Potential Exclusions after Initial Identification

After MasterCard identifies a merchant in the GMAP, the acquirer has an opportunity to provide additional data and information to MasterCard for review and consideration of an exclusion. MasterCard performs all reviews conducted for this purpose on a case-by-case basis.

To request consideration for an exclusion, the acquirer must provide the documentation that MasterCard requires within 30 days of the merchant identification. If the acquirer does not provide the documentation, MasterCard will list the merchant name and location in a *Global Security Bulletin* with the applicable chargeback liability period.

MasterCard staff will use its discretion on the decision to exclude a merchant identification or to require additional action by the acquirer, such as a decision to accept chargeback liability or to terminate the merchant agreement.

When MasterCard does not grant an exclusion, it will list the merchant name and location in a *Global Security Bulletin* with the applicable chargeback liability period.

When reviewing exclusion requests, MasterCard will consider the following:

- *Fraud-to-sales ratio exceeds 100%*—MasterCard will exclude such merchants temporarily, until MasterCard reviews on a case-by-case basis. When additional action is required, MasterCard will notify the acquirer and provide 30 days for the acquirer to respond.
- *Fraud-to-sales ratio below 1%*—If an identified merchant's actual MasterCard volume is not systematically available for calculation, an acquirer will have the opportunity to provide this data to MasterCard for review. To recalculate the merchant fraud-to-sales 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.

  When the supporting documentation demonstrates that the merchant location did not exceed the program thresholds, the acquirer will receive an exclusion for the merchant.

  When the supporting documentation demonstrates that the fraud-to-sales ratio at the merchant location exceeds 1%, MasterCard will require the acquirer to comply with the actions in Figure 5.3, based on the value of fraud-to-sales ratio.
- *Chain stores*—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 the same 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.

  Members with a merchant listed in GMAP based on a calculation inclusive of more that 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. 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.

If an acquirer fails to provide the requested documentation or the requested documentation fails to show that the transactions occurred at more than one location, MasterCard may deny an exclusion request and require the acquirer to accept chargeback liability or to terminate the merchant agreement.

Acquirers that successfully provide the data necessary to show that each merchant location did not exceed the program thresholds will receive an exclusion for the merchant.

- *One-time merchant exclusion*—If the fraud-to-sales ratio and fraud volume of an identified merchant is not of an egregious nature and extenuating circumstances exist, MasterCard may, at staff discretion, provide a one-time exclusion.

  An acquirer must request this type of exclusion by providing the necessary documentation to support each case. The following are examples of circumstances where MasterCard would consider an exclusion:

  - 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)
  - The merchant captured fraudulent card(s) transacted at its location.
  - The merchant assisted with the apprehension and conviction of criminal(s) that transacted fraudulent cards at its location.
  - 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.

8.4.6 Notification of Merchant Identification

When a merchant location is identified in the GMAP, MasterCard will send a GMAP advisory letter to the acquirer, detailing the identification and specifying the required member response.

In addition to the letter, the acquirer will receive the Global Merchant Audit Program Report. Members must use MOST to respond to merchant identifications in the GMAP.

Note

MasterCard 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®.

8.4.6.1 Distribution of Reports

MasterCard offers acquirers the option of receiving the GMAP reports via mail, through the Banknet network, or via eService and Fraud Reporter on MasterCard OnLine.

Reports are generated on or about the second calendar day of every month and available on the same day to members using eService or Fraud Reporter on MasterCard OnLine®. MasterCard will send reports sent via mail and the Banknet network to members on or about the sixth calendar day of the month.

The file specifications for the GMAP reports sent via the Banknet® telecommunications network are shown in Figure 8.3.

Figure 8.3—Banknet File Specifications for GMAP Reports

Element		Description
Bulk ID	=	T831
Sequence Number	=	00
Record Length	=	133 characters
Block size	=	931 characters

1. The file for the reports contains seven records to a block and is transmitted in a print image format.
2. The first character contains the ASA carriage control characters.
3. The remaining 132 characters contain the actual print line.

To change the report endpoint or the member contact information for the GMAP, members should contact the Customer Operations Services team:

Phone: 1-800-999-0363 or 1-636-722-6176 (English language support)
1-636-722-6292 (Spanish language support)

Fax: 1-636-722-7192

E-mail: member_support@mastercard.com (Canada, Caribbean, and United States)
local contact information (Asia/Pacific)
css@mastercard.com (Europe)
emeaap@mastercard.com (South Asia/Middle East/Africa)
lagroup@mastercard.com (Latin America)

8.4.7 Merchant Online Status Tracking (MOST) System

The MasterCard Merchant Online Status Tracking (MOST) system resides on the MasterCard OnLine® platform, and is used to administer the process for merchants identified in the GMAP. The MOST system allows an acquirer to:

- View each merchant identified in the GMAP
- Determine the reasons a merchant was identified in the GMAP
- Retrieve full transaction details for each identified merchant
- View the status of the identified merchants, including any exclusion or request for additional information
- Submit electronic responses directly to MasterCard in a timely manner
- Determine the applicable chargeback liability period for each merchant identified in Tier 3 of the GMAP

8.4.7.1 MOST Mandate

Members must use the MOST system available on MasterCard OnLine for responding to MasterCard about merchants identified in the GMAP. Members do not pay a registration fee or other fees to access and use MOST. However, MasterCard will assess a USD 100 processing fee per individual merchant identification on a member that does not solely use MOST to submit initial merchant responses.

MasterCard will assess the USD 100 processing fee only one time for each merchant identification. The fee will be collected by debiting the member's MCBS account.

In addition, MasterCard may assess an acquirer a USD 100 processing fee if the same communication is submitted in duplicate via MOST and using any other additional method. However, if an acquirer sends the initial response 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.

8.4.7.2 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. A user must submit the required product registration request via MasterCard OnLine. The user also must provide the necessary written authorization from the Principal, Security, or MasterCard MATCH™ system contact listed in the *Member Information Manual* (MIM) for the respective member ID.

MasterCard will decline requests for access to the MOST system that are not accompanied by the required authorization. When MasterCard declines a request, the user must resubmit a subsequent online product registration request in addition to supplying written authorization.

To register for MOST, navigate your browser to www.mastercardonline.com and select **Order Product** from the menu bar at the left of your screen. You will be directed to the online *MasterCard Product Catalog*, where you will locate **Merchant Online Status Tracking (MOST)** and then select **New Product Request**.

To update a user's existing MOST license, follow the navigation instructions above, but choose **Update Product Access** instead of the **New Product Request**.

For additional assistance in registering for the MOST online system, you may contact Online Solutions and Services using one of the following methods:

Phone:	1-800-737-5019 (Canada and United States)
Phone:	1-636-722-2095 (All regions)
Fax:	1-636-722-22039
E-mail:	online_requests@mastercard.com

8.6 Excessive Chargeback Program

The Excessive Chargeback Program applies to all merchants and is designed to reduce excessive chargebacks, excessive credits to cardholder accounts, and fraud.

It is the acquirer's responsibility to monitor its merchants on an ongoing basis, in accordance with the requirements set forth in section 7.2 of this manual. Should the acquirer determine that a merchant exceeded the Excessive Chargeback Program thresholds, it must immediately notify the MasterCard Merchant Fraud Control department and declare the merchant an Excessive Chargeback Merchant.

Should a merchant, or a merchant location, have a minimum of 15 chargebacks and a ratio of chargeback transactions to total sales transactions of at least 1%, or a ratio of chargeback dollar volume to sales dollar volume of at least 2.5% for two consecutive calendar months, then MasterCard staff may, at its discretion, declare the merchant, or a specific location of the merchant, to be an Excessive Chargeback Merchant.

8.6.1 Credits

When, in the opinion of MasterCard staff, the merchant has issued credits for any of the reasons or conditions listed below or to otherwise avoid the applicability of this rule, MasterCard will consider the credits as chargebacks in evaluating the merchant's performance. For example:

- Credits issued in lieu of chargebacks, either before or after the initiation of the chargeback
- Credits issued because of the merchant's failure to control its backroom processes
- Credit issued exceed the number of chargebacks received by the merchant
- Refunds issued by means of a check to resolve fraud or customer service issues

MasterCard may assess the acquirer USD 25 for each credit processed, in addition to any chargeback assessments.

8.6.2 Acquirer Liability

Once a merchant is declared an Excessive Chargeback Merchant, the acquirer(s) of record is liable for issuer recovery costs related to chargebacks and credits (if applicable), as described in section 8.6.6.1 and any other applicable fees and assessments from the period during which the Excessive Chargeback Program thresholds were exceeded. A change to the corporation status, business name, or ownership of an Excessive Chargeback Merchant will not affect the applicability of these rules.

If MasterCard identifies a merchant under the Excessive Chargeback Program and the acquiring relationship ends and the merchant subsequently enters into a new acquiring relationship, MasterCard reserves the right to transfer the chargeback recovery cost liability and any other applicable fees and assessments to any new acquirer for the applicable period. MasterCard will base the applicable period on information in the MATCH system and published in the *Global Security Bulletin*. The new acquirer must register the identified merchant with MasterCard, as described in section 8.6.3 before processing transactions.

8.6.3 Registration

MasterCard will identify merchants exceeding the Excessive Chargeback Program thresholds in a *Global Security Bulletin*. The acquirer must register such merchants within 15 calendar days of the *Global Security Bulletin*. For registration requirements, refer to section 9.4.4 of this manual.

MasterCard will assess the acquirer an annual USD 1,000 registration fee for each merchant identified under the Excessive Chargeback Program. MasterCard will collect the fee from the acquirer via MCBS.

8.6.3.1 Noncompliance Assessments for Failure to Register and for Excessive Fraud

If the acquirer fails to register an Excessive Chargeback Merchant or if an Excessive Chargeback Merchant exceeds USD 25,000 in fraud in any calendar month, the acquirer will be subject to the assessments described in section 9.4.5.

8.6.4 MasterCard Evaluation

MasterCard will evaluate transaction data to determine whether the Excessive Chargeback Program thresholds were exceeded. MasterCard will notify affected acquirers formally, in writing, of the evaluation outcome.

If a subsequent MasterCard evaluation of a merchant previously declared an Excessive Chargeback Merchant determines continuing performance issues at the original or new acquirer, MasterCard may extend the assessments and the issuer recovery cost period beyond the dates initially indicated in the original *Global Security Bulletin*.

8.6.5 MasterCard Post-evaluation Procedure

If MasterCard declares a merchant, or a merchant location, in violation of the Excessive Chargeback Program, MasterCard will notify the acquirer and directly debit its MCBS account for the appropriate amount.

Staff then will list the merchant in a *Global Security Bulletin* and notify issuers of the period during which they can charge back transactions.

8.6.7 Recurring Payment Transaction Processing Prohibition for Electronic Commerce Adult Content (Videotext) Merchants

If MasterCard determines that an electronic commerce adult content (videotext) merchant is identified in the Excessive Chargeback Program, MasterCard will notify the acquirer and will list the identified merchant in a *Global Security Bulletin*. The acquirer must not submit into interchange a recurring payment transaction for a one-year period, effective from the first day of the month following the acquirer's notification.

If an Excessive Chargeback Merchant terminates its relationship with the acquirer, MasterCard will transfer the prohibition for processing recurring transactions to any new acquirer for the applicable period.

8.6.7.1 Acquirer Noncompliance

In addition to the assessments described in section 9.4.5, the acquirer is subject to an assessment of up to USD 25,000 per month per merchant when the acquirer fails to prohibit an electronic commerce adult content (videotext) merchant from processing recurring transactions.

9.1 Merchant Registration Program Overview

MasterCard requires the registration of the following merchant types and other entities under the Merchant Registration Program (MRP), using the Merchant Registration Program system, available through MasterCard Online:

- Key-entry telecom merchants (refer to section 9.4.1)
- Electronic commerce adult content (videotext) merchants (refer to section 9.4.3)
- Merchants identified under the Excessive Chargeback Program (refer to section 8.6)
- Entities required to implement the MasterCard Site Data Protection Program (refer to section 10.5)

If a member acquires transactions for any of these merchant types without first registering the merchant in accordance with the Standards described in this section, MasterCard may assess the member as set forth in section 9.4.5. In addition, the acquirer must ensure that the violation is corrected promptly.

Refer to chapter 3 of the *Security Systems Specifications* manual for technical information about the use of the Merchant Registration Program.

9.2 Registration Requirements

The acquirer must provide the following information for each merchant or Third Party Processor (TPP) to be registered under the Merchant Registration Program:

- The name, doing business as (DBA) name, and address of the merchant or TPP
- The central access phone number, customer service phone number, or e-mail address of the merchant or TPP
- The name(s), address(es), and tax identification number(s) (or other relevant national identification number) of the principal owner(s) of the merchant or TPP
- A detailed description of the service(s) that the merchant or TPP will offer to cardholders

- A description of payment processing procedures, cardholder disclosures, and other practices including, but not limited to:
  - Data solicited from cardholder
  - Authorization process (including floor limits)
  - Customer service return policies for card transactions
  - Disclosure made before soliciting payment information
  - Data storage and security practices
- The identity of any previous business relationship(s) involving the principal owner(s) of the merchant or TPP
- A certification, by the officer of the acquirer with direct responsibility to ensure compliance of the registered merchant or TPP with MasterCard Standards, stating that after conducting a diligent and good faith investigation, the acquirer believes that the information contained in the registration request is true and accurate

Only MasterCard can modify or delete information about a registered merchant or TPP. Acquirers must submit any modification(s) about a registered merchant or TPP in writing to MasterCard, with explanation for the request. MasterCard reserves the right to deny a modification request.

Acquirers should send any additional requested information and modification requests to the Vice President of Merchant Fraud Control at the address provided in Appendix E.

For registration requirements specific to merchants, TPPs, and Data Storage Entities (DSEs) in the e-commerce environment that are required to implement the MasterCard Site Data Protection Program, refer to section 10.5 of this manual.

9.3 Monitoring Requirements

The monitoring requirements described in this section apply to members that acquire key-entry telecom transactions, electronic commerce adult content (videotext) transactions, or transactions from merchants identified 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 MasterCard card account number
  - Consecutive or excessive attempts using the same MasterCard card account number

  When attempted fraud is evident, a merchant should implement temporary BIN blocking as a fraud deterrent.
- Every three months, effective one calendar month from the date of such merchant's registration with MasterCard, the acquirer must submit to MasterCard (via the Merchant Registration Program) a report of sales, chargeback, and credit activity by calendar month.

9.4 Additional Registration and Monitoring Requirements

Members 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 MasterCard 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.

9.4.1.1 Registration and Monitoring

Before an acquirer may process key-entered telecom transactions from a merchant, it must register the merchant with MasterCard.

The acquirer must ensure that the key-entry telecom merchant complies with the fraud control Standards and maintains a total chargebacks-to-interchange sales volume ratio below the Excessive Chargeback Program thresholds. For information on the Excessive Chargeback Program, refer to section 8.6.

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 must notify MasterCard (through the Merchant Registration Program system) of each of its key-entry telecom merchant with a chargebacks-to-interchange sales volume ratio exceeding 1% (transaction count) or 2.5% (dollar amount) for any two consecutive months. The acquirer must notify MasterCard by the 15th day of the month immediately following the two consecutive months in which the ratio exceeds these thresholds.

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 MasterCard 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, use MCC 7276 (Dating and Escort Services). For merchants that rent adult content videotapes and DVDs, use MCC 7841.

9.4.3.1 Registration and Monitoring

Before an acquirer may process electronic commerce adult content (videotext) transactions from a merchant, it must register the merchant with MasterCard. MasterCard assesses the acquirer an annual USD 1,000 registration fee for each of its electronic commerce adult content (videotext) merchants. MasterCard will collect the fee from the acquirer via the MasterCard Consolidated Billing System (MCBS).

The acquirer must ensure that the electronic commerce adult content (videotext) merchant complies at all times with the fraud control and other Standards and maintains a total chargebacks-to-interchange sales volume ratio below the Excessive Chargeback Program thresholds, defined as chargebacks-to-interchange sales volume ratio of 1% (transaction count) or 2.5% (dollar amount) for any two consecutive months. The acquirer must notify MasterCard, through the Merchant Registration Program system, of each of its electronic commerce adult content (videotext) merchants that exceeds these thresholds. The acquirer must notify MasterCard by the 15th day of the month immediately following the two consecutive months in which the ratio exceeds the established thresholds. For more information about the Excessive Chargeback Program, refer to section 8.6.

9.4.4 Merchants Identified Under the Excessive Chargeback Program

MasterCard will identify merchants exceeding the Excessive Chargeback Program thresholds in a Global Security Bulletin. The acquirer must register such merchants within 15 calendar days of the *Global Security Bulletin*.

MasterCard will assess the acquirer an annual USD 1,000 registration fee for each merchant identified under the Excessive Chargeback Program. MasterCard will collect the fee from the acquirer via MCBS.

9.4.5 Noncompliance Assessments for Failure to Register and for Excessive Fraud

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

If, after notice by MasterCard of its failure to register a merchant, the acquirer fails to do so within 10 days, MasterCard may assess the acquirer up to USD 25,000 for each calendar month until the acquirer satisfies the requirement. In addition, the acquirer must ensure that the violation is corrected promptly.

Additionally, if an electronic commerce adult content (videotext) merchant or a merchant identified in the Excessive Chargeback Program exceeds USD 25,000 in fraud in any calendar month, the acquirer will be subject to the additional assessments in Figure 9.1.

Figure 9.1—Noncompliance assessments

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

[a] Months may be non-consecutive.

10.1 Card and Cardholder Data Protection Standards

Members must store all media containing MasterCard cardholder and account information, including such data as account numbers, personal identification numbers (PINs), credit limits, and account balances, in a secure area, complying with the requirements mentioned in section 2.1 of this manual and section 3.7 of the MasterCard *Bylaws and Rules* manual. Further, access to the secured area must be limited to selected personnel on a "need-to-have-access" basis. Before discarding any such media, destruction must be in a manner that will render account data unreadable. Members must limit and control access to account data stored in computers, terminals, and PCs by establishing data protection procedures that include but are not limited to a password system for Computer Remote Terminal (CRT) access and control over dial-up lines or any other means of access.

MasterCard cards, embossed or unembossed, should be stored in a vault or controlled storage room. Issuers must destroy discarded cards by cutting or shredding, or by any other means that will render them unusable.

10.1.1 Working with Third Parties

Issuers delivering media with account information to agent processors must ensure that such processors adhere to the in-house procedures except that, at the member's option, the media may be returned to the member rather than destroyed. Any media, printed or otherwise, delivered to credit bureaus or other outside agencies that provide services to a member should contain only that portion of an account number necessary for identifying an account. Bank identification numbers (BINs) and filler numbers may be deleted or the account number scrambled.

10.2 Transaction Data Protection Standards

This section describes Standards for the processing and storage of MasterCard transaction and account information by acquirers or merchants or any agent or representative thereof (including Third Party Processors (TPPs) and Data Storage Entities (DSEs)). Refer to section 9.15 of the *Bylaws and Rules* manual for additional Standards relating to the storage of account, cardholder, transaction, and merchant information by merchants and DSEs.

10.2.1 Card-read Data Storage Standards

The following rules and restrictions apply for the display and storage of card-read data:

- A terminal or other device at the point of interaction must not display, replicate, or store any card-read data except card account number, expiration date, service code, and cardholder name, if present.
- The acquirer, the merchant, or any agent representative thereof (including TPPs and DSEs), may record only the card account number, expiration date, service code, and cardholder name on paper, microfiche, or an online authorization file, in a secure environment to which access is limited, solely for research or exception processing purposes at its site. The issuer may request a copy of the data that is retained for such purposes. The acquirer, the merchant, or any agent representative thereof (including TPPs and DSEs) may retain or replicate no other transaction data. Acquirers that currently store full card-read (including discretionary) data for the sole purpose of providing documentation for exception processing must discontinue such storage as soon as practical, but no later than 1 October 2005.

MasterCard strongly recommends that acquirers review the procedures and systems, and those of their merchants, DSEs, agents, and representatives to ensure compliance with these Standards.

At its discretion, MasterCard may impose a noncompliance assessment for failure to comply with these requirements, as described in section 9.5.2.3 of the *Bylaws and Rules* manual.

10.2.2 CVC 2 Data Storage Standards

Acquirers, merchants, or any agent representative thereof (including TPPs and DSEs), and any POI terminals or devices operated by any such entity, must not store CVC 2 data in any manner for any purpose. Issuers should not expect CVC 2 data in recurring transaction Authorization Request/0100 messages.

At its discretion, MasterCard may impose a noncompliance assessment for failure to comply with these requirements, as described in section 9.5.2.3 of the *Bylaws and Rules* manual.

10.2.3 Use of Wireless Local Area Network (LAN) Technology

Acquirers, merchants, TPPs, and DSEs that use wireless LAN technology to connect networks or servers that process or store MasterCard transaction or account data must comply with all of the following requirements:

1. Wi-Fi protected access (WPA) technology must be implemented for encryption and authentication when the wireless LAN technology is WPA-capable. Use of a Virtual Private Network (VPN) also is recommended.
2. When the wireless LAN is not WPA-capable, a VPN must be implemented.
3. Wireless Equivalent Privacy (WEP) must not be the sole method used to protect confidentiality and access to a wireless LAN.

For more information about wireless LANs and the WPA security protocol, refer to *Wireless LANs—Security Risks and Guidelines*, available through the Member Publications tool on MasterCard OnLine®.

10.3 Account Data Compromise Events

MasterCard periodically receives information about accounts that may have been exposed to a compromise that, in turn, potentially could lead to unauthorized use of the cardholder account. This section sets forth procedures and requirements in the event that any member, merchant, DSE, or TPP becomes aware of a possible account data compromise.

10.3.1 MasterCard Evaluation

MasterCard will evaluate the totality of known circumstances with respect to the potential compromise, including any actions taken by the compromised party to establish, implement, or maintain procedures and support best practices to safeguard account data. The determination of any assessments and related costs will be at the sole discretion of MasterCard.

10.3.2 Acquirer Responsibilities

When an acquirer becomes aware of an account data compromise event or a suspected event, the acquirer must take the following action:

- Conduct an investigation and promptly provide results to MasterCard.
- On an ongoing basis, obtain and provide to MasterCard the list of compromised, or possibly compromised, account numbers.
- Take immediate action to ensure the security of the suspected compromised entity(ies) and MasterCard account data.

In addition, aquirers must take the following action:

- Within 24 hours of its knowledge of an account compromise:
  - Notify the MasterCard Compromised Account Team by e-mail at compromised_account_team@mastercard.com or by phone at 1-636-722-4100;
  - Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via e-mail, to compromised_account_team@mastercard.com; and
  - Provide Merchant Fraud Control staff with the complete list of all known compromised account numbers.
- Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
- Provide weekly written status reports to MasterCard, addressing open questions and issues, until the audit is complete to the satisfaction of MasterCard.
- Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.

- Provide forensic reports and findings of all audits and investigations to Merchant Fraud Control staff within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

The acquirer(s) of record at the time of the suspected compromise will be held fully responsible for achieving resolution of all outstanding issues and liabilities to the satisfaction of MasterCard, notwithstanding any change in its relationship with the compromised party(ies). In the event of a dispute regarding this obligation, MasterCard, in its sole discretion, shall determine the acquirer(s) of record and related responsibilities.

10.3.3 Notification to Affected Issuers

After obtaining the details of the account data compromise and the list of compromised account numbers, MasterCard will:

- Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs
- Distribute the account number data to its respective issuers

MasterCard may publish a *Global Security Bulletin* or other communication to alert issuers about the compromise and the rights and obligations arising in connection therewith.

10.3.5 Additional Requirements for the E-commerce Environment

For an acquirer to be eligible for a reduction of MasterCard noncompliance assessments or related reimbursement costs in the event of an account data compromise, acquirers must have registered the e-commerce merchant or TPP suspected to have been compromised as compliant with the PCI Data Security Standard. For more information about the PCI Data Security Standard, refer to section 10.5 of this manual.

The requirements in this section apply only to the e-commerce environment and apply to acquirers, merchants, and TPPs.

10.3.5.1 Compliance with Security Standard

MasterCard requires acquirers to provide any documents that substantiate compliance with the PCI Data Security Standard at the time of the compromise.

If MasterCard determines that an e-commerce merchant or TPP registered as compliant with the PCI Data Security Standard is found to be out of compliance with that standard, MasterCard will modify the registration of that entity pursuant to section 10.5. MasterCard will require re-registration once all vulnerabilities identified are resolved, at which time MasterCard again will assess the applicable registration fee, according to section 10.5.6 of this manual.

10.3.6 Noncompliance Assessments

If the account compromise was a result of a violation of MasterCard Standards regarding disclosure and securing of cardholder account and transaction data, the member may be subject to noncompliance assessments. As set forth in sections 9.5.2 and 9.15 of the *Bylaws and Rules*, MasterCard may assess up to USD 100,000 for each violation, with a maximum aggregate assessment of USD 500,000 for additional or continuing violations during any consecutive 12-month period.

If the member fails to comply with the procedures set forth in section 10.3.2 of this manual, MasterCard may impose an additional assessment of up to USD 25,000 each day until the member achieves compliance. Continued, extended, or repeated noncompliance may lead to the suspension or termination of the violating party's participation in the MasterCard payment system.

In addition to the assessments indicated above, MasterCard may assess all investigation and other related costs incurred by MasterCard against the acquirer. With regard to accounts identified as potentially compromised, MasterCard may require the acquirer to reimburse affected issuers, as described in section 10.3.4.

10.3.6.1 Potential Exemption from Noncompliance Assessments

MasterCard may exempt the acquirer from noncompliance assessments and/or MasterCard investigative costs, and other related costs; and MasterCard, at its sole discretion, may grant up to a 100% reduction from the issuer reimbursement costs. MasterCard will base any exemption or reduction that may be afforded on the totality of the circumstances, including whether the compromised party was registered properly as in compliance with the PCI Data Security Standard at the time of the compromise.

Among the circumstances that MasterCard will consider when determining an exemption or reduction afforded are the following:

- Verification that the registration of the compromised merchant or TPP, pursuant to chapter 9 and section 10.5.6 of this manual and chapter 7 of the *Bylaws and Rules*, was current at the time of the compromise.
- Substantiation to MasterCard of compliance with the PCI Data Security Standard by the compromised merchant or TPP.
- Demonstration by a data security firm's network security scan report and MasterCard Security Self-assessment results of the successful remediation of risks and compliance before the compromise. Refer to section 10.5.2 of this manual.
- Notification to and cooperation with MasterCard and, as appropriate, law enforcement authorities.
- Verification that the forensics examination was initiated within 72 hours of the compromise and completed as soon as practical.
- Timely receipt of the forensics examination findings.
- Evidence that the compromise was not foreseeable or preventable by commercially reasonable means and that, on a continuing basis, best practices were applied.

MasterCard generally will not grant an exemption or reduction for an internal compromise, which is a compromise facilitated by persons authorized to have access to the system or process compromised. In addition, following any such exemption or reduction, the compromised party must maintain compliance with the PCI Data Security Standard after satisfactorily addressing the identified security concerns.

10.4 Common Point of Purchase (CPP) Investigations

MasterCard will identify merchant locations at which MasterCard account data may have been compromised and subsequently used to effect fraudulent transactions at other points of interaction. MasterCard will denote each such merchant location as a common point of purchase (CPP).

Issuers may request that MasterCard initiate an investigation of a merchant for possible CPP activity at any time. Acquirers have five business days to acknowledge a request from MasterCard for a CPP investigation. Acquirers have 30 calendar days to complete the investigation. Failure to respond may result in fines or assessments.

Only MasterCard, not a member, may designate a merchant location as a CPP and request that an acquirer conduct a CPP investigation in accordance with the CPP program requirements. MasterCard will identify a merchant location as a CPP from one or more of the following sources:

- Information received from law enforcement and investigative authorities;
- Issuers in accordance with the criteria set forth below (see Issuer Investigation Request, section 10.4.1 below); **and**
- MasterCard systems, databases, and any other source deemed to be reliable.

10.4.1 Issuer Investigation Request

Issuers may request that MasterCard require a CPP investigation of a particular merchant location. To place an investigation request, the issuer must complete and submit section A of the CPP Referral Form found on MasterCard Alerts by identifying and listing at least three genuine transactions (at least one of which must be a MasterCard transaction) involving different account numbers that each were used at a merchant and subsequently used for fraudulent activity. The three or more transactions all must have occurred within a 90 calendar day period, and the oldest transaction must have occurred within a 180 calendar day period of the CPP investigation request.

For each subsequent fraudulent transaction, and for each such previous transaction, the issuer must:

- Examine the Authorization Request/0100 message log (or an equivalent data element for American Express, Visa, or other payment activity) to determine whether the acquirer transmitted the full magnetic stripe data during the authorization process; **and**
- Determine whether an authorized cardholder had physical possession of the card(s) at the time of each such transaction.

The issuer also must provide all of the following information:

- Issuer name, member ID, requestor's name, phone number, fax number, and e-mail address
- Acquirer member ID or bank identification number (BIN)
- The merchant name and location of the possible CPP
- Additional information about the transactions at the possible CPP, including account numbers, transaction amounts, transaction dates, times of authorization, and skimming period time frame

- Details about all fraudulent transactions, including account numbers, transaction amounts, and transaction dates
- Issuer contact request selection, indicating that the issuer would like to be contacted prior to the commencement of the acquirer's investigation
- An explanation of the basis for the issuer's belief that the merchant location may have been the source of compromised account data

The issuer must submit the completed CPP Referral Form to the MasterCard Alerts administrator via the MasterCard Alerts™ system.

Note **If members have internal documents containing any of the information requested on the CPP Referral Form, they can attach these documents and submit them, along with their completed CPP Referral Form, via MasterCard Alerts.**

10.4.2 MasterCard Action

MasterCard will review the CPP Referral Form to determine whether the issuer provided all the required information. If not, MasterCard will return the form to the issuer for completion and resubmission. Once the form has been completed, MasterCard will review the sufficiency of the information provided in section A and determine whether to forward the CPP Referral Form via MasterCard Alerts to the acquirer, together with a request that the acquirer conduct an investigation.

MasterCard Alerts obtains its contacts through licensed users of the MasterCard Alerts System and the *Member Information Manual* (*MIM*). Therefore, it is crucial that all information in the MIM be kept up to date at all times. Additionally, communication is directed to the Primary Contact, Security Contact, and Merchant Acquirer Contact with each CPP.

MasterCard will maintain an electronic file to reflect CPP program action. Member access to the file will be limited to the following information to complete the investigation or update the electronic form:

- Indication that a CPP investigation has been requested with respect to a merchant location. This indication will remain available to members until the investigation is completed or MasterCard determines that the indication should be removed from the file; **and**

- Indication that a CPP investigation has been completed with respect to a merchant location. This notice will remain available to members for 30 days following the date that MasterCard determines the investigation to be complete.

All information is disseminated through MasterCard Alerts. Information will not be accepted by any other means, such as e-mail or fax. Should MasterCard have to disburse information outside of the MasterCard Alerts System, each instance will have associated assessments of USD 1,000.

Note

It is the sole responsibility of each member institution, not MasterCard, to have up-to-date and complete information listed in the *MIM*.

MasterCard will not waive any assessments associated with noncompliance due to insufficient or incorrect information listed in the *MIM*.

10.4.3 Acquirer Response

In response to a CPP investigation request, the acquirer must comply with all of the following requirements:

- Using MasterCard Alerts, acknowledge the request for a CPP investigation by completing section B of the CPP Referral Form within five business days of receiving the request
- Complete the investigation and submit section C of the CPP Referral Form to the MasterCard Alerts administrator within 30 days of receiving the request via MasterCard Alerts
- Provide all required background, financial, and other information about the CPP to the MasterCard Alerts administrator
- Report the results of the investigation such as whether the account data was improperly disclosed, by whom, in what manner, and what remedial action was taken
- Ensure that the merchant does not store or release account data information contradictory to the Standards, and if so, that remedial action promptly is taken
- Implement Security and Risk Services staff directives aimed at identifying the cause and any individual responsible for the data compromise
- Cooperate fully with law enforcement investigation, if any
- Cooperate fully with any resulting or subsequent prosecution

Final CPP investigation results will be acceptable for 30 calendar days from the close of the CPP investigation in the event additional issuer requests of the same merchant are received. After the 30-day time frame, a new investigation should be completed in order to determine whether suspicious activity is ongoing.

Note

Requests for extensions in order to finalize investigation results must be made at least one week before the final due date of the investigation. Extensions are granted at the sole discretion of MasterCard.

MasterCard will determine whether to continue to designate the merchant location a CPP.

The acquirer must take additional action when MasterCard receives a subsequent unique CPP investigation request within 30 to 180 days of the original CPP investigation request. In that case, MasterCard requires the acquirer to complete a site inspection and fulfill all due diligence requirements described in this section report within 30 days of notification of the subsequent CPP investigation request. The site inspection due diligence report must consist of the following information:

- The date and merchant location of the site inspection
- A summary of the actions that the merchant took to investigate the CPP event
- The findings related to the CPP event investigation
- Documentation of any preventative measures put in place as a result of the CPP event

The acquirer must draft send a letter and send the letter to the CPP administrator stating that the required due diligence is complete. The acquirer must provide the site inspection report as an attachment to the letter.

10.4.3.1 Acquirer Noncompliance

MasterCard may assess an acquirer for failure to comply with CPP responsibilities. MasterCard may deem each failure a separate violation for assessment purposes. Multiple violations can result from a single CPP investigation request. For example, if an acquirer fails to acknowledge receipt of an investigation request and also fails to initiate an investigation, then MasterCard may cite the acquirer for two noncompliance violations.

MasterCard also may request additional information from the acquirer after the completed investigation date. A due date will be established at the time of the request, based on the content of the information requested. Should the acquirer fail to acknowledge or respond to the information request, MasterCard may assess acquirers for noncompliance. Each CPP will be reviewed on an individual basis.

With each incident of noncompliance, a certified or registered letter, fax, or e-mail with confirmation will be sent to the acquirer's Security Contact, Principal Contact, and Merchant Acquirer Contact.

In cases of acquirer noncompliance, the assessments in Figure 10.1 apply.

Figure 10.1—Noncompliance Assessments

Acquirer Noncompliance	Assessment
First violation	None
Second violation	MasterCard may subject the acquirer to a Level 3 RAMP review (USD 10,000), and may impose an assessment of up to USD 15,000.
Third violation	MasterCard may assess the acquirer up to USD 20,000, and may refer the incident to the Audit Committee of the MasterCard Global Board of Directors for review and recommendation.
Fourth and all further violations	MasterCard may assess the acquirer up to USD 25,000, and refer the incident to the Audit Committee of the MasterCard Global Board of Directors for review and recommendation.

MasterCard will debit all assessments and reimbursements directly from the acquirer's MasterCard settlement account.

10.5 MasterCard Site Data Protection (SDP) Program

The MasterCard Site Data Protection (SDP) Program is designed to encourage members, merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect themselves and all participants in the system against the threat of account data compromises. SDP facilitates the identification of vulnerabilities in security processes, procedures, and Web site configurations.

Acquirers must implement the MasterCard SDP Program by ensuring that their merchants, TPPs, and associated DSEs, are compliant with the Payment Card Industry (PCI) Data Security Standard in accordance with the implementation schedule defined in section 10.5.5. Going forward, the PCI Data Security Standard will be a component of SDP; the PCI Data Security Standard sets forth security standards that MasterCard hopes will be adopted as industry standards across the payment brands.

A member that complies with the SDP Program requirements may qualify for a reduction, partial or total, of certain costs or assessments if the member, a merchant, a TPP, or a DSE is the source of an account data compromise.

Refer to section 10.2.3 of this manual for requirements on the use of wireless local area network (LAN) technology by members, merchants, TPPs, and DSEs.

Definition **Data Storage—The temporary or permanent retention of MasterCard account data in any form (including logs) for subsequent processing, retrieval, or other use.**

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

Definition **Data Storage Entity (DSE)—An entity other than a member, merchant, or MSP that stores, transmits, or processes MasterCard account data, transaction data, or both on behalf of a member, merchant, or MSP. Examples of DSEs include, but are not limited to, Web hosting companies, payment gateways, terminal drivers, software providers, and processors.**

10.5.1 Payment Card Industry (PCI) Data Security Standard

The MasterCard SDP Program establishes data security requirements and best practices specified in the PCI Data Security Standard. The PCI Data Security Standard is applicable to every member and other person or entity a member permits, directly or indirectly, to access or store account data.

The PCI Data Security Standard manuals are available in the Member Publications product of MasterCard OnLine®, as well as on the MasterCard SDP Program Web site at https://sdp.mastercardintl.com.

10.5.2 Security Evaluation Tools

As defined in the implementation schedule in section 10.4.2, merchants, TPPs, and DSEs must use the following evaluation tools:

- On-site Reviews—The onsite review evaluates a merchant's, TPP's, or DSE's compliance with the PCI Standard. Onsite reviews are an annual requirement for Level 1 merchants and for Level 1 and 2 service providers. Merchants may use an internal auditor or independent assessor recognized by MasterCard as acceptable. TPPs and DSEs must use an acceptable third-party assessor as defined on the SDP Program Web site.
- The Security Self-assessment—The Security Self-assessment is a questionnaire available at no charge on the MasterCard SDP Program Web site. To be compliant, each Level 2, 3 and 4 merchant, and each Level 3 DSE 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, all TPPs, and all DSEs as required by the implementation schedule must conduct scans on a quarterly basis using a vendor listed on the SDP Program Web site. To be compliant, scanning must be conducted in accordance with the guidelines contained in the PCI Data Security Standard documents and the *Security Scanning Requirements for Vendors* manual.

10.5.3 Vendor Compliance Testing

As part of the MasterCard SDP Program, MasterCard provides a vendor compliance testing process for vendors that provide network scanning services. Technical requirements for network scanning vendors are provided in the *Payment Card Industry Security Scanning Procedures*. For more information about this service, acquirers should visit the MasterCard SDP Program Web site at https://sdp.mastercardintl.com.

At this Web site, MasterCard will also post a listing of all acceptable onsite assessors for the purposes of meeting the onsite review requirement.

10.5.4 Acquirer Compliance Requirements

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

- Submit to the attention of the MasterCard Site Data Protection Department or e-mail to sdp@mastercard.com by 31 December of the previous calendar year:
  - A list of all merchants, TPPs, and DSEs that must comply with the PCI Data Security Standard during each phase of the SDP Program mandate.

    For each merchant, TPP, and DSE, acquirers must provide:
    - The name and primary address of each merchant, TPP, and DSE
    - The merchant identification number for each merchant
    - For each merchant, the name of each TPP and DSE that stores MasterCard account data on the merchant's behalf
    - For each merchant, the number of transactions processed during the previous 12-month period
- Deploy an SDP security compliance program for all applicable merchants, TPPs, and DSEs in accordance with the implementation schedule detailed in section 10.5.5
- Ensure that merchants, TPPs, and DSEs comply with the requirements of the security evaluation tools detailed in section 10.5.2
- Register merchants, TPPs, and DSEs affected by the implementation schedule in accordance with the registration requirements detailed in section 10.5.6.

10.5.5 Implementation Schedule

All onsite reviews, network security scans and self-assessments must be conducted according to the guidelines in section 10.5.2. For purposes of the SDP Program, Service Providers in this section refer to TPPs and DSEs.

Level 1 Merchants

The following entities must be SDP compliant:

- All merchants that have suffered a hack or an attack that resulted in an account data compromise,
- All merchants, including e-commerce merchants, with greater than six million total transactions annually,
- All merchants exceeding the Level 1 criteria of a competing payment brand, and
- Any merchant that MasterCard, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system.

To be compliant, Level 1 merchants successfully must complete:

- An annual onsite review by either the merchants' internal auditor or by an independent security assessor, and
- Quarterly network scans.

Level 2 Merchants

The following entities must be SDP compliant:

- All merchants with between 150,000 and 6 million annual e-commerce transactions, and
- All merchants exceeding the Level 2 criteria of a competing payment brand.

To be compliant, Level 2 merchants successfully must complete:

- An annual self-assessment, and
- Quarterly network scans.

Level 3 Merchants

The following entities must be SDP compliant:

- All merchants with between 20,000 and 150,000 annual e-commerce transactions, and
- All merchants exceeding the Level 3 criteria of a competing payment brand.

To be compliant, Level 3 merchants successfully must complete:

- An annual self-assessment, and
- Quarterly network scans.

Level 4 Merchants

SDP is optional for all other merchants. SDP compliance is recommended strongly for Level 4 merchants to reduce the risk of compromise and for acquirers to potentially gain a waiver against account data compromise assessments.

To be considered compliant, Level 4 merchants successfully must complete:

- An annual self-assessment, and
- An annual network scan.

Level 1 Service Providers

Level 1 service providers include all acquiring TPPs and all DSEs that store data on behalf of Level 1 and Level 2 merchants.

All Level 1 service providers must be SDP compliant. Compliance by this date includes successful completion of:

- An annual self-assessment, and
- Quarterly network scans.

All Level 1 service providers must accomplish the following to be considered SDP compliant:

- Successful completion of an annual onsite review by an independent security assessor, and
- Successful completion of quarterly network scans.

Level 2 Service Providers

Level 2 service providers include all those DSEs that store data on behalf of Level 3 merchants.

Level 2 service providers must accomplish the following to be considered SDP compliant:

- Completion of an annual onsite review by an independent security assessor, and
- Completion of quarterly network scans.

Level 3 Service Providers

Level 3 service providers are all other DSEs not included in Levels 1 and 2. SDP compliance is optional for Level 3 service providers.

SDP compliance, however, is recommended strongly to reduce the risk of compromise and for acquirers to potentially gain a waiver against account data compromise assessments.

To be considered compliant, Level 3 service providers successfully must complete:

- An annual self-assessment, and
- Quarterly network scans.

MasterCard will monitor the SDP Program and has the right to audit member compliance. Noncompliance on or after the required implementation date may result in the following assessments:

Failure to comply with the SDP Program mandate within…	Will result in an assessment, per merchant, TPP, or DSE of…
6 months	Up to USD 2,000
18 months	Up to USD 5,000
36 months	Up to USD 25,000 per year

Should MasterCard determine that an acquirer has not complied with any SDP Program mandate, MasterCard may assess such acquirer up to USD 100,000 for a first violation and up to USD 500,000 in aggregate for any continuing violation during a continuous 12-month period.

10.5.6 SDP Program Registration

Annual registration of merchants, TPPs, and DSEs is the responsibility of the acquirer and must be completed using the Member Registration Program available on MasterCard OnLine®. Acquirers must register separately each applicable merchant, TPP, and DSE.

By registering a merchant, TPP, or DSE as SDP compliant, the acquirer certifies that:

- The merchant, TPP, or DSE has engaged and used the services of a data security firm(s) that is considered acceptable by MasterCard for onsite audit evaluations and/or security scanning.
- By review of the audit, self-assessment, or network scan reports, the acquirer has determined compliance with the PCI Data Security Standard requirements.
- On an ongoing basis, the acquirer will monitor compliance. If found to be noncompliant, the acquirer must notify the MasterCard SDP Department in writing at sdp@mastercard.com.

For general registration requirements, refer to section 9.2.

The acquirer must, as part of the registration process:

- Identify if the entity being registered is a merchant or a TPP or DSE
- Provide the name and location of the merchant or TPP or DSE being registered and such other information as MasterCard may request from time to time
- Provide merchant or TPP or DSE principal data as MasterCard may request from time to time
- If registering a merchant, indicate whether the merchant stores account data
- If registering a merchant, identify any TPP that performs transaction processing services, as defined in chapter 7 of the *Bylaws and Rules*.
- For the merchant's registration to be valid, the TPP already must be registered as SDP-compliant by the acquirer
- If registering a merchant, identify any DSE that stores account data on behalf of the merchant. For the merchant's registration to be valid, the DSE already must be registered as SDP-compliant by the acquirer.

The acquirer must register each merchant, TPP, and DSE in accordance with the implementation schedule detailed in section 10.5.5.

When considering if a merchant stores 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 data temporarily in memory files. Per the MasterCard data storage definition, temporary or permanent retention of account data is considered to be storage. Merchants that do not store data never process 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.

MasterCard will assess the acquirer an annual USD 200 registration fee for each merchant that stores account data. However, for each merchant that does not store data, the appropriate TPP, DSEs, or both must be identified for the merchant's registration to be valid. Before identifying the TPP, DSE, or both, the acquirer already must have registered the TPP, DSE, or both as compliant.

MasterCard will assess an acquirer the USD 200 fee for each TPP and each DSE registered by that acquirer.

Regardless whether the TPP or DSE was registered previously by a different acquirer, MasterCard will collect the registration fee from the acquirer via MCBS.

11.1 MATCH Overview

MasterCard designed MATCH™, the Member Alert to Control High-risk (Merchants) system, to provide acquirers with the opportunity to develop enhanced or incremental risk information before entering into a merchant agreement. MATCH is a mandatory system for MasterCard 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 inaccuratly 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 member-reported information about merchants and their owners to offer acquirers the following fraud detection features and options for assessing risk:

- Acquirers may add and search for information about 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 all data and reduces processing delays by notifying inquiring members of errors as records are processed.
- MATCH supports retroactive alert processing of data residing on the database for up to 120 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 120 days. The inquiring acquirer must then determine whether additional investigation is appropriate, or if it should take other measures to address risk issues.

Refer to chapter 1 of the *Security Systems Specifications* manual for technical information regarding the use of MATCH.

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 120 days.

MATCH searches for possible exact matches and possible phonetic 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 emplyed and the inability to report a true and exact match with absolute certainty.

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.

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, two, or three—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 been reported to the Acquirer at least once within the past 120 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:

Figure 11.1—Exact Possible Match Criteria

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

[a] If country is USA

[b] If country is not USA

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

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."

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

Figure 11.2—Phonetic Possible Match Criteria

Field	+	Field	+	Field	=	Match
Business Name					=	✓
Doing Business As (DBA) Name					=	✓
Business Street Address	+	City	+	State [c]	=	✓ ✓
Business Street Address	+	City	+	Country [d]	=	✓ ✓
Principal Owner's (PO) First Initial	+	Last Name			=	✓
PO Street Address (lines 1 and 2)	+	PO City	+	PO State [c]	=	✓ ✓
PO Street Address (lines 1 and 2)	+	PO City	+	PO Country [d]	=	✓ ✓

[c] If country is USA

[d] If country is not USA

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

11.2 MATCH Standards

MasterCard mandates that all acquirers with merchant activity use MATCH. To use means both to:

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

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

11.2.1 Certification

Each MasterCard 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 many send and receive MATCH records to and from MasterCard.

Warning **An acquirer that conducts merchant acquiring activity 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 Figure 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 Figure 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 Figure 11.4 must be met or suspected (at decision to terminate) to justify a merchant addition.

An acquirer that fails to enter a merchant to 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 9.2.1 of the *Bylaws and Rules*.

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 Figure 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.

The MATCH system database stores inquiry records for 120 days.

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.

D.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 MasterCard card transactions, including physical dimensions, weight, color, carbon paper, registration marks, numbering, standard wording, and printing.

D.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.

D.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.

D.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.

D.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).

D.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 members 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:

- 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

D.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 ± 0.010 inches 0(.0762 cm ± 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 (± 2 degrees).

D.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 ± 0.050 inches (± 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.

D.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.

D.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 ± 0.040 inches (0.557 cm ± 0.102 cm) from the top of the formset.

D.1.8 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."

D.1.9 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.

D.2 Formset Printing Standards

The Standards listed below apply to the printing of formsets.

D.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 D.1.9 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 (see the "Registration Mark" discussion in this chapter), 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.

D.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 left edge and 0.970 inches (2.468 cm) from the top edge of the slip.
   - 0.875 inches (2.224 cm) long by .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 .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.

D.2.3 Imprinters

Each member 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 MasterCard 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 member disbursing the cash disbursement, and the city and state (or country, if the location is outside the United States) where the transaction occurred.

6 *Excerpts from* Maestro Global Rules *(published July 2005)*

This chapter contains excerpts of the Maestro Global Rules *manual published July 2005. This* Merchant Rules Manual *contains only information applicable to merchants; therefore, some sections provided in the* Maestro Global Rules *manual may have been omitted herein.*

3.1 Compliance

Participants must comply with the Rules, and the regulations, policies and technical specifications of the Organization as may be in effect from time to time.

Members are responsible for ensuring the compliance of their agent(s), and Merchant(s).

3.7 Record Retention

During the term of participation and for two (2) years after termination of participation, each Participant agrees to receive and hold in confidence any and all materials or information considered proprietary or confidential by any other Participant.

For the purposes of this section of the Rules, confidential information includes, without limitation, the following:

a. information concerning technical practices in implementing and operating the Organization;

b. information concerning the entity under consideration for membership in the Organization, prior to public disclosure;

c. Transaction volume and any other statistical information relating to the operation of the Organization;

d. Identity Standards;

e. information concerning applications, specifications, licenses, operating systems, and value-added data on Chip Cards.

Participants must retain records of Transactions communicated to or by it, for a period as specified by applicable governmental regulation, but in no case less than two (2) years.

Merchants must retain a copy of Transaction printouts for a period as specified by applicable governmental regulation, but in no case less than two (2) years. Within the retention period, Acquirers must produce a copy of a Transaction receipt upon request.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

4.2 Use of the Service Marks

A Member must not use or authorize another to use any of the Service Marks (including, without limitation, the interlocking circles device owned by MasterCard) in any manner except in strict compliance with the Rules, and the regulations, policies, and the Identity Standards of the Organization, and pursuant to the terms and conditions of its Maestro License Agreement, as same may be amended from time to time.

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

The Organization reserves the right to determine, establish and control the nature and quality of the services rendered by its Participants under any marks it adopts.

Members must use the Service Marks in the manner prescribed in the Identity Standards for all applications, including, but not limited to, uses on Cards, POI Terminals, signage, correspondence, and advertising.

A Member may use the Service Marks as a stand-alone, incremental or cross-border brand for its Cardholders, at the discretion of its Maestro Regional Licensor.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

4.2.2 Cessation of Participation

Any Member that ceases to participate in the Organization must:

a. stop issuing Cards and distributing materials incorporating any Service Marks, on the date it gives notice that it is leaving the Organization, or on the date it is given notice of termination;

b. have replaced all Cards bearing any Service Marks, no later than the date of leaving the Organization;

c. remove any Service Marks from all POI Terminals locations on the date it leaves the Organization.

Upon termination from the Organization, a Member must promptly return to the Organization all systems and confidential information that are proprietary to the Organization and all materials displaying any Service Marks.

The Acquirer must ensure that its Merchant ceases all use of the Service Marks and promptly returns any materials displaying the Service Marks immediately upon termination of the Merchant Agreement.

A terminated Merchant must promptly return all materials displaying the Service Marks to the Acquirer.

Note **For further information about withdrawal from the Organization, refer to chapter 1, "Introduction and Participation Requirements," of this rulebook.**

Note **A regional rule variation on this topic appears in chapter 17, "Asia/Pacific Region," of this rulebook.**

4.4 Display of the Service Marks at POI Terminals

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," and chapter 22, "United States Region," of this rulebook.**

Members must display the Service Marks in accordance with the Rules, and the regulations, policies and Identity Standards of the Organization as may be published from time to time, within thirty (30) calendar days of the POI Terminal's first Transaction.

Members must not display signage in a false, deceptive or misleading manner.

All signage used by a Member with respect to the Service Marks must comply with all applicable laws, Rules, and the regulations, policies, and Identity Standards of the Organization.

The Service Marks may not be placed on or near, or otherwise used to identify any POS Terminal, which does not accept Cards.

Maestro Regional Licensors may permit or prohibit the display of the logo of a Competing EFT POS Network at POS Terminals.

4.4.1 New and Replacement Signage

All new and replacement signage, other than signage used to comply with section 4.4 of the Rules, referring to POI Terminals that participate in the Organization must comply with this subsection 4.4.1. On any new or replacement signage incorporating the marks of a competing network, the corresponding Service Marks must appear and be given at least equal prominence. The Service Marks must be at least as large as the marks of any competing network.

4.5 Protection of the Service Marks

Members must assist the Organization in whatever manner is reasonably necessary to protect the Organization's and others' rights in the Service Marks and other marks to which reference is made in section 4.2.

Members must not threaten or initiate any litigation relating to the Service Marks and such other marks, without first obtaining the consent of the Organization.

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

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

5.1 Applicability of the Standards

The rules set forth in this chapter apply to all Affinity/Co-Brand programs (A/CB programs). An A/CB program involves the placement on Cards of a trade name, mark, or both, of any entity or group not eligible to become a Member (the A/CB partner). The intent of these A/CB rules is to prevent an A/CB partner from enjoying the benefits of membership without being a Member.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

5.5 Acceptance Requirements

5.5.1 Accept All Cards without Discrimination

Subject to the Standards, each Acquirer and Merchant must accept Cards equally and without discrimination. Therefore, all POI Terminal locations that accept an A/CB Card, including any Merchants owned and/or controlled by an A/CB partner, must also accept all other Cards without limitation or exception.

5.5.2 Use of the Service Marks

The Service Marks must be displayed on a stand-alone basis apart from any A/CB partner identification at any POI Terminal that accepts Cards.

The Service Marks displayed at the POI Terminal must at least have parity in size and prominence with any A/CB logo program name and competing payment systems mark also displayed.

The Organization has the right to require the modification of any POI Terminal display of an A/CB program name or logo that the Organization determines does not comply with these Rules or adversely affects the Service Marks.

The A/CB program Card face design may not be used as an element of any Merchant decal.

5.6 Discounts on Purchases—Europe Region and Latin America and the Caribbean Region Only

Note **Regional rules on this topic appear in chapter 19, "Europe Region," and chapter 20, "Latin America and the Caribbean Region," of this rulebook.**

5.7 Compliance with Prepaid Card Program Requirements

An Issuer of a prepaid Card Program must comply with the terms set forth in the document entitled Policy for MasterCard, MasterCard Electronic, Maestro, and Cirrus Prepaid Card Programs, which is located on MasterCard OnLine.

5.7.1 Communication Standards

All solicitations, applications, advertisements, disclosures, and other material and information (including Web sites) regarding any prepaid Card Program (collectively for the purposes of this chapter only, "Solicitations") must refer prominently to the offering as a prepaid Card—they may not position the offering as something other than a prepaid Card—and must be submitted to the Organization for review and approval prior to the prepaid Card Program's launch and prior to any marketing of the prepaid Card Program.

Any Solicitation regarding any prepaid Card Program must prominently and integrally feature the Service Marks and must identify the Issuer.

A Solicitation may not imply or state that anyone other than the Member is the Issuer of the prepaid Card.

Each Solicitation for a prepaid Card must clearly and conspicuously disclose and identify all features associated with that prepaid Card Program.

7.1 Acquirer Obligations and Activities

7.1.1 Signing a Merchant—POS and Electronic Commerce Only

7.1.1.1 The Merchant Agreement

Each Acquirer must directly enter into a written merchant agreement with each Merchant from which it intends to acquire Transactions, whether such Transactions are submitted to the Acquirer by the Merchant, or through a Member Service Provider (MSP) acting for or on behalf of such Acquirer.

An Acquirer must not submit for processing any Transaction arising in connection with any commercial entity that makes goods or services available to Cardholders for purchase with a Card, unless the commercial entity has a valid merchant agreement with the Acquirer. This rule applies regardless of whether the ability to use the Card is explicit or implied, or whether the Card is presented directly to the commercial entity, a third-party processor, or any other person. A commercial entity is any person that sells goods or services

on an ongoing basis, and that maintains a physical or virtual presence for the purpose of selling goods or services.

If an Acquirer uses an MSP, the Acquirer must itself execute a written agreement directly with each Merchant. The agreement must reflect the Acquirer's primary responsibility for the Merchant relationship, and must otherwise comply with these Standards.

When the Rules are amended, each Acquirer is responsible for making any necessary and appropriate amendments to its form of merchant agreement.

The Merchant's right to use or display the Service Marks continues only as long as the merchant agreement remains in effect. Refer to chapter 4, "Service Marks," for further information about the use and display of the Service Marks.

7.1.1.2 Required Provisions

Each merchant agreement must contain the substance of each of the Standards set forth in the Rules, and be applicable to the nature and manner of the Merchant's business. The failure to include the substance of any one or more of such Standards in the merchant agreement or the grant of a waiver or variation with respect to one or more of these provisions does not relieve a Member from chargebacks or compliance proceedings.

Each merchant agreement must contain a provision that sets forth payment terms agreed upon by the Member and the Merchant, addressing when the Member will pay the Merchant for Transactions received from the Merchant, as required by the Standards.

The merchant agreement may contain additional terms and conditions that are mutually agreed upon between the Acquirer and the Merchant, provided such terms and conditions do not conflict with any provisions contained in these Standards, and other rules, regulations and policies of the Organization.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.1.1.3 Acquirer Responsibility for Merchant Compliance

The Acquirer is responsible for ensuring that each of its Merchants complies with the Rules and technical specifications of the Organization, and is jointly and severally liable with its Merchants for each of the Merchant obligations in the merchant agreement.

The Acquirer must take appropriate actions that may be necessary or appropriate to ensure the Merchant's compliance, such as reviewing the Merchant's deposit records and procedures for effecting Transactions. Failure to comply with any of the Standards may result in chargebacks, a penalty to the Acquirer, or other disciplinary action.

7.1.2 Before Signing a Merchant

7.1.2.1 Verify Bona Fide Business Operation

Before entering into, extending, or renewing a merchant agreement, the Acquirer must verify that the Merchant from which it intends to acquire Transactions is a bona fide business, and that the Transactions will reflect bona fide business between the Merchant and the Cardholder.

In addition, the Acquirer must review the Merchant's activity to determine if it engages in the processing of special Transaction types (see chapter 9, "Processing Requirements"). Special Transaction processing requirements apply to wire transfer money orders, quasi cash, gaming Transactions and truck stop Transactions. The Acquirer and the Merchant must comply with all Standards applicable to these special Transactions. This requirement applies if a merchant agreement exists and the Merchant wishes to expand its activities to include these Transactions.

a. The Acquirer must at a minimum:

   1. investigate the Merchant's previous merchant agreement(s);
   2. review the Merchant's most recent annual report, including the audited financial information, if the Merchant is a company listed on a stock exchange and has annual sales in excess of USD 50 million (or the foreign currency equivalent);
   3. review the Merchant's most recent audited financial statement, if the Merchant is a privately owned company and has annual sales revenue in excess of USD 50 million (or the foreign currency equivalent);
   4. follow good commercial banking practices where the review of the annual report or audited financial statement would suggest additional inquiry.

b. If current audited financial information is unavailable or if the Merchant is government-owned or has annual sales revenues of USD 50 million or less (or the foreign currency equivalent), the Acquirer must:

   1. Inspect the Merchant's premises and records to ensure that it has proper facilities, equipment, inventory, agreements, and licenses required 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; and

   2. Conduct a credit check or other background investigation to determine the financial condition of the owner, if the Merchant is a sole proprietorship. If a credit check raises questions regarding the creditworthiness of the Merchant, then a credit check must be conducted of:

      a. The principal shareholders and principal offices if the Merchant is a corporation; or

      b. The partners if the Merchant is a partnership; or

      c. The parent corporation if the Merchant is a subsidiary.

The Organization has the right to audit an Acquirer's records to determine compliance with these Standards.

These Merchant signing requirements do not apply to the extent that compliance would violate local law. The Organization may approve a recognized local alternative to a requirement if the alternative provides substantially the same level of protection to the Organization.

7.1.3 Acquiring Transactions

Before acquiring Transactions and on an on-going basis thereafter, the Acquirer must test to ensure that appropriate procedures, technology, software, hardware, and control devices are in place to properly complete Transactions, without undue risks to other Members, Cardholders, or Merchants.

The Acquirer must ensure that the Merchant informs the Cardholder that the Merchant is responsible for the Transaction, including the goods or services that are the subject of the Transaction, and for related customer service, dispute resolution, and performance of the terms and conditions of the Transaction.

It is the Acquirer's responsibility to ensure that all channels that process Transactions comply with the Rules, and the regulations, policies and technical specifications of the Organization. The Acquirer must perform tests, both initially and on an on-going basis to ensure compliance with this rule. Refer to chapter 3, "Common Obligations," for further information.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.1.5 Transmitting and Processing Transactions

Acquirers must maintain, directly or indirectly, a functional twenty-four (24)-hours-per-day operating connection to the Interchange System.

Acquirers must transmit all Transactions they acquire online to the Interchange System, in accordance with the applicable Standards. Refer to chapter 9, "Processing Requirements," for additional information.

If there is no agreement for the transmission and processing of domestic Transactions, Acquirers must use the format and procedures for Cross-Border Transaction processing as described in the technical specifications for the Interchange System.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.1.6 Card Acceptance Requirements

Each Acquirer must ensure that:

a. it actively promotes the Organization;

b. the Service Marks, in color, are prominently displayed at all POI Terminals, and on promotional materials, in accordance with the Standards, to inform the public that Cards will be honored;

c. the Service Marks are displayed at least in the same size and place as any competing acceptance brand;

d. all valid Cards are honored without discrimination when properly presented by Cardholders at any POI Terminal displaying the Service Marks. Cards must be honored on terms no less favorable than the terms under which other cards are accepted. A Merchant that does not deal with the public at large (for example, a private club) is considered to comply with this rule if it honors Cards of Cardholders that have purchasing privileges with the Merchant;

e. a Merchant does not require, or post signs indicating that it requires a minimum or maximum Transaction amount to accept a valid Card;

f. a Merchant does not refuse to complete a Transaction solely because a Cardholder who has complied with the conditions for presentment of a Card at the POI refuses to provide additional identification information, except as specifically permitted or required by the Rules;

g. if IIN/BIN files are received and used for Transaction routing and processing, that such files are input and available for use, within six (6) calendar days from the date that the updated IIN/BIN table is distributed;

h. any Card that conforms with the encoding Standards is accepted as a valid Card;

i. the confidentiality and security of PINs entered into PIN-entry devices are assured. All POS Terminals and Terminals must be able to encrypt PINs at the point of entry, and send them to the host computer in encrypted form as required by applicable Standards. Refer to chapter 8, "Security," for further information;

j. all required Transaction types are supported, as described in chapter 9, "Processing Requirements," of this rulebook;

k. all valid Transactions are accepted and processed in accordance with the Standards;

l. the Cardholder is given the opportunity to receive a receipt, which must comply with the Standards and all applicable laws and regulations. The PAN must be truncated on any Transaction receipt issued. (Refer to the receipt and PAN truncation requirements later in this chapter for further information);

m. Merchants prominently and unequivocally inform Cardholders of the identity of the Merchant at all points of interaction, so that the Cardholder readily can distinguish the Merchant from any other party, such as a supplier of goods or services.

7.1.7 Record Retention

Acquirers 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 the agreement is terminated.

In addition, Acquirers must retain a record of each Transaction communicated to or by it, for a minimum of two (2) years, or such longer period as may be required by applicable law, rule, or regulation. Refer to chapter 3, "Common Obligations," for further information.

During the required retention period for POS Transactions, Acquirers must produce a copy of a Transaction receipt, upon request.

7.1.8 Transaction Inquiries and Disputes

Acquirers must ensure the provision and support of processes to facilitate the handling of Transaction inquiries, disputes, Transaction documentation requests, and chargebacks.

7.1.9 Audit Trails

Acquirers must ensure that audit trails are maintained, from which it will be possible to identify any violation of the Rules or the existence of any significant risk to the Organization.

7.1.11 Quality Assurance

From time-to-time, the Organization will perform quality audits to ensure Card acceptance. Acquirers are required to participate in such audits, and must follow the procedures as established by the Organization from time-to-time, and published to Members.

7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant

POS and Electronic Commerce Only

In addition to the requirements documented in section 7.1, on an ongoing basis, each Acquirer must:

a. ensure that each of its Merchants is provided with all materials necessary to effect Transactions in accordance with the Standards, and to signify Card acceptance. These materials may include POS Terminals, PIN pads, advertising displays, Merchant decals, and other point-of-interaction promotional materials bearing the Service Marks;

b. monitor its Merchants' compliance with the Rules and technical specifications of the Organization, including checking for and testing out Merchant contact details. If requested by the Organization, the Acquirer must take any action that may be necessary or appropriate to ensure the Merchant's compliance with the Rules. This action may include terminating Merchants whose practices pose a risk to the Interchange System;

c. acquire all Transactions properly presented to it from each of its Merchants on such terms as set forth in the merchant agreement between them;

d. exercise deposit monitoring and other fraud controls to identify suspicious Merchant activity. The Acquirer must ensure that its Merchant presents only valid Transactions between itself and a bona fide Cardholder. The Merchant must not present Transactions that it knows, or should have known to be fraudulent, or not authorized by the Cardholder. Within the scope of this rule, the Merchant is responsible for the actions of its employees;

e. be satisfied that the Merchant is able to support the fulfillment of the products and/or services to be marketed;

f. ensure that the Merchant has procedures and resources to handle Cardholder inquiries and to support refunds, where necessary;

g. provide the respective Merchant/outlet descriptions within each Transaction record;

h. ensure that the Merchant assigns an account for the crediting and debiting of Transactions, and for the debiting of items charged back;

i. credit or debit (as applicable) the Merchant's designated bank account with the amount, (either gross or net of merchant discount) of all Transactions. This obligation is not discharged until the Merchant receives payment from the Member, notwithstanding any Member payment arrangement, including any such arrangement between an Affiliate Member and its Principal Member. An Acquirer may, by agreement of the Merchant, withhold amounts for chargeback reserves or similar purposes.

j. ensure Merchants and their DSEs keep all systems and media containing Card, Cardholder, or Transaction information (whether physical or electronic) in a secure manner to prevent access by or disclosure to any unauthorized party. The Merchant and its DSE must destroy, in a manner that will render the data unreadable, all such media that the Merchant no longer deems necessary or appropriate to store. The Merchant and its DSE may store Card, Cardholder, or Transaction information only to the extent specified in the Standards;

k. ensure that Merchants promptly inform the Acquirer of the name of any DSE that engages in, or proposes to engage in, the processing and/or storage of Card data for the Merchant, whether directly or indirectly, regardless of the manner or duration of such activities;

l. ensure that Merchants prominently and unequivocally inform the Cardholder of the identity of the Merchant at all points of interaction so that the Cardholder readily can distinguish the Merchant from any other party such as a supplier of goods or services to the Merchant;

m. ensure that Merchants immediately notify the Acquirer of an Account compromise. Refer to section 7.2.2 for additional information;

n. ensure that the Merchant does not sell, purchase, provide, exchange or in any manner disclose Account number information or a Cardholder's name to anyone other than to its Acquirer, to the Organization, or in response to a government request.

Note **An additional regional rule on this topic appears in chapter 17, "Asia/Pacific Region," of this rulebook.**

7.2.1 Storage of Account, Cardholder, and Transaction Data

Upon receipt of an Authorization Request Response message for a Transaction, the Merchant and any of its DSEs must not store certain information contained in the Authorization Request message and Authorization Request Response message in any system. This information includes discretionary card-read data, PIN data, or any other prohibited information as set forth in the Rules.

7.2.2 Account Data Compromise Event

When an Acquirer becomes aware of a Card data compromise event or a suspected event, the Acquirer must take the following action:

a. conduct an investigation and promptly provide results to the Organization;

b. on an ongoing basis, obtain and provide to the Organization the list of compromised, or possibly compromised, Account numbers;

c. take immediate action to ensure the security of the suspected compromised entity(ies) and Card data;

d. within 24 hours of its knowledge of an Account compromise:

   1. notify the MasterCard Compromised Account Team via phone at 1-636-722-4100;

   2. provide a detailed written statement of fact about the Account compromise (including the contributing circumstances) via e-mail, to compromised_account_team@mastercard.com; and

   3. provide the MasterCard Merchant Fraud Control Department with the complete list of all known compromised Account numbers.

e. within 72 hours of knowledge of a suspected Account compromise:

   1. engage the services of a data security firm acceptable to the Organization to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation);

   2. provide weekly written status reports to the Organization, addressing open questions and issues, until the audit is complete to the satisfaction of the Organization;

   3. promptly furnish updated lists of potential or known compromised Account numbers, additional documentation, and other information that the Organization may request; and

   4. provide findings of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of the Organization.

The Acquirer(s) of record at the time of the suspected compromise will be held fully responsible for achieving resolution of all outstanding issues and liabilities to the satisfaction of the Organization, notwithstanding any change in its relationship with the compromised party(ies). In the event of a dispute regarding this obligation, the Organization, in its sole discretion, will determine the Acquirer(s) of record and related responsibilities.

The Acquirer must cooperate with the investigation and resolution of the Card compromise, including any forensic audit or other measure that the Organization deems necessary in its sole discretion.

If the Account compromise was a result of a violation of the Rules regarding disclosure and securing of Cardholder, Card and Transaction data, the Acquirer may be subject to noncompliance assessments. If the Acquirer fails to comply with the procedures set forth in this section 7.2.2, the Organization may impose additional assessments against the Acquirer until the Acquirer achieves compliance. Refer to chapter 16, "Noncompliance Assessments," for additional information. In addition, the Organization may assess against the Acquirer all investigation and other related costs incurred by the Organization.

7.2.3 Merchant Surcharging

Unless permitted by local laws or regulations, Acquirers must ensure that their Merchants do not require Cardholders to pay a surcharge or any part of any Merchant discount, or any contemporaneous finance charge in connection with a Transaction. A Merchant may provide a discount fee to its customers for cash payments.

A Merchant is permitted to charge a fee (such as commission, postage, expedited service or convenience fees, and the like), if the fee is imposed on all like transactions regardless of the form of payment used.

Note **A regional rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

7.2.4 Merchant Noncompliance

The Organization will notify an Acquirer if the Acquirer or the Acquirer's Merchant fails to comply with the Rules.

The Organization may require action to eliminate the deficiencies, require the Acquirer to suspend or discontinue Organization activities with the Merchant concerned, or levy noncompliance assessment fees.

7.2.5 Refinancing of Previously Existing Debt and/or Payment of Bad Debts—Asia/Pacific Region Only

Note **Regional rules on this topic appear in chapter 17, "Asia/Pacific Region," of this rulebook.**

7.4 Acquiring Electronic Commerce Transactions

An Acquirer can acquire electronic commerce Transactions on a global basis for any Merchant with a business location in the same Region as the Acquirer.

An Acquirer can also acquire electronic commerce Transactions on a global basis for any Merchant that does not have a business location in the Acquirer's Region, if the Acquirer follows the acquiring regulations defined by the Maestro Regional Licensor of the Region in which the Merchant has its business location.

For the purposes of determining the appropriate interchange fee and an Acquirer's right to acquire a particular Merchant, the location of the Merchant is defined as the Merchant's address as documented in the merchant agreement between the Acquirer and the Merchant.

This address may be based on the location of the Merchant's physical premises, the jurisdiction where the Merchant pays taxes, the currency used by the Merchant, or some other place. Any disagreement among Members as to a Merchant's location may be referred to the Organization for resolution.

Note **A regional rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

7.4.1 Acquirer Responsibilities: Electronic Commerce Transactions

In addition to the requirements documented in sections 7.1, 7.2 and 7.4, Acquirers must ensure that all Merchant sites that accept electronic commerce Transactions:

a. clearly display the Service Marks on the Web site. The method and size used to display the Service Marks must be at least equal to the method and size used for displaying other payment marks, and must be in accordance with brand standards;

b. are capable of accepting PANs between thirteen (13) and nineteen (19) digits in length;

c. support the passing of the data in UCAF to the Acquirer. Refer to the *MasterCard SecureCode Member Enrollment and Implementation Guide* (MSG) for further information;

d. support 3D Secure Merchant Plug-in, and are capable of handling Transactions within a 3D Secure environment. Refer to the MSG for further information;

e. provide a set of "help" functions to help Cardholders that have not yet been enabled by their Issuers for transacting via the Internet. Refer to the MSG for a list of valid "help" functions;

f. follow best practices in the display of price information, ensuring Cardholders can clearly identify the amount of currency of the Transactions that they are authorizing;

g. display details of the timing of billing and fulfillment of Transactions.

An Acquirer must provide each Merchant with a Merchant ID, and ensure that its Merchants correctly populate all UCAF fields with required data elements.

On an on-going basis, the Acquirer must educate electronic commerce Merchants to ensure that they understand the special risks and responsibilities associated with accepting Transactions in an electronic environment.

7.4.1.1 Merchant Requirements: Electronic Commerce Transactions

Each Merchant must:

a. clearly display a mailing address, and a contact telephone number or e-mail address, for customer queries resulting from electronic commerce Transactions. This information may be displayed on any page within the Merchant's Web site, but must be readily accessible to a Cardholder, and remain displayed for at least ninety (90) calendar days after the last day on which a Transaction was performed;

b. name and format the UCAF hidden fields in accordance with the MSG and technical specifications of the Organization;

c. have the capability to accept PANs between thirteen (13) and nineteen (19) digits in length;

d. populate a hidden form field (the UCAF Brand field) on its purchase page to signify that the Merchant accepts Maestro as a method of payment. This allows the wallet to "wake-up." Refer to the MSG for further information;

e. ensure that the order confirmation section of the Merchant's Web page contains UCAF hidden fields that are not visible to the Cardholder, but which are readable by the Issuer Wallet Server (IWS). Refer to the MSG for further information;

f. provide a function for Cardholders to confirm a purchase on the Web site. This confirmation function must be provided before the sale has been completed and any charges levied;

g. display a receipt page, after the Cardholder confirms a purchase. The display of the receipt on the screen must be printable;

h. ensure that information provided on any e-mail acknowledgement of the Cardholder's order is in compliance with all other requirements for a Transaction receipt. Refer to receipt requirements later in this chapter for further information;

i. not request an authorization until the goods or services are ready to be dispatched. Refer to chapter 9, "Processing Requirements," for further information about processing electronic commerce Transactions;

j. ensure that the Transaction amount used in the authorization message matches the value of the goods in an individual shipment, including any additional charges for posting and packing etc.;

k. ensure that the combined amount of all shipments does not exceed the total amount agreed with the Cardholder. The Merchant must send an e-mail notification to the Cardholder explaining that the order will be sent in more than one shipment, and that a payment will be requested for each shipment;

l. ensure that the Cardholder is advised if, as a result of Multiple or Partial Deliveries the original price is exceeded or the total completion of the order has taken more than thirty (30) calendar days from the time the Cardholder placed the order. The Merchant will then be required to make a new purchase order for the additional amount and, if appropriate, include the revised delivery date. This new Transaction must be authorized and processed in accordance with the Rules and technical specifications of the Organization.

7.5 Acquiring Payment Transactions

a. Only Acquirers and Merchants approved and registered by the Organization to effect Payment Transactions may do so.

b. Acquirers must always submit a postable authorization request to the receiving Issuer for all Payment Transactions.

c. The Acquirer or Merchant must present the Payment Transaction on or before the date agreed to with the recipient Cardholder.

d. The Acquirer or Merchant must not aggregate two (2) or more funds transfers or payments into a single Payment Transaction. In addition, the Acquirer or Merchant may not divide one Payment Transaction into many.

e. In a dual message environment, Acquirers must submit a clearing message to the Interchange System within twenty-four (24) hours of the authorization request.

f. The Acquirer must not submit a reversal or adjustment to correct a clerical error made while conducting a Payment Transaction. Any requests by the Acquirer to correct a clerical error will be approved or rejected at the discretion of the Issuer.

g. Acquirers or Merchants who offer the Payment Transaction service must not request or require that a Cardholder disclose his or her PIN.

   If the Payment Transaction service is provided via a Web page, the Merchant must not design that Web page in any way that might lead the Cardholder to believe that he or she must provide his or her PIN. Similarly, if the Cardholder is asked to complete a form in order to conduct a Payment Transaction, the contents of that form must not lead the Cardholder to believe that he or she must provide his or her PIN.

   The Acquirer must ensure that the Merchant is following these procedures. The Organization will also, from time to time, perform audits on these Merchants to ensure that they are compliant with this and all other requirements.

h. The Acquirer or Merchant must not effect a Payment Transaction in order to transfer the proceeds from a Transaction to a commercial entity or to another Merchant.

7.5.1 Member Registration Procedures for Payment Transactions

A Payment Transaction may be submitted for processing, only by Members or Merchants that are registered by the Organization. When determining whether to register a Member or Merchant, the Organization will consider several factors, including but not limited to, the following:

a. Member compliance with the Rules and systems requirements;

b. adequate Payment Transaction disclosure to Cardholders (for example, disclosure of transactional limitations, such as per-day maximum Payment Transaction limits that apply across all payment methods);

c. appropriate Cardholder experience (for example, Cardholder procedures for inquiries and disputes); and

d. Member financial control and risk management procedures.

The Organization will monitor programs on an ongoing basis. In its sole discretion, the Organization may rescind its approval and Member or Merchant registration at any time.

7.6 Eligible POI Terminals

The following types of terminals are eligible to be POI Terminals as applicable:

a. any ATM that is owned, operated or controlled by a Member, and that is capable of complying with all of the applicable provisions of the Rules, and the regulations, policies and technical specifications of the Organization;

b. any ATM that is owned, operated or controlled by an entity that is ineligible to be a Member, provided that such ATM is connected to the Interchange System by a Principal or Affiliate Member and is capable of complying with all the applicable provisions of the Rules, and the regulations, policies and technical specifications of the Organization. Refer to chapter 14, "Member Service Providers," for additional information;

c. any POS Terminal that is owned, operated or controlled by a Merchant, provided that such POS Terminal is connected to the Interchange System by a Principal or Affiliate Member and further provided that such POS Terminal is capable of complying with all the applicable provisions of the Rules, and the regulations, policies and technical specifications of the Organization. Refer to section 7.1.1 as set forth in this chapter;

d. any other type of terminal which the Organization may authorize.

All POI Terminals must be identified by the appropriate Service Marks pursuant to the Rules, and the regulations, policies and Identity Standards of the Organization.

Note **A regional rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

7.6.1 Ineligible Terminals

All terminals that dispense scrip must be disconnected from the Interchange System no later than 1 December 2003.

Acquirers are prohibited from sponsoring into the Organization new terminals that dispense scrip.

7.7 POS Terminal and Terminal Requirements

All eligible POS Terminals and Terminals must:

a. perform Transactions only after receiving authorization from the Issuer or from the Chip Card;

b. read and transmit all track 2 data encoded on the Card's magnetic stripe for authorization;

c. provide operating instructions in English as well as the local language;

d. ensure privacy of PIN entry to the Cardholder;

e. have a screen display that enables the Cardholder to view the data (other than the PIN), entered into the POS Terminal or Terminal by that Cardholder, or the response received as the result of the Cardholder's Transaction request. This data will include the application labels or preferred names on a multi-application Card, and the amount of the Transaction. Refer to chapter 8, "Security," for the security requirements; and

f. prevent additional Transactions from being entered into the system while a Transaction is being processed.

Note **Additional regional rules and a regional rule variation on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.7.1 Card Reader

POS Terminals and Terminals must have a magnetic stripe reader capable of reading track 2 data encoded on Cards.

7.7.2 Manual Key-Entry of PAN

Transactions must not be performed if neither the magnetic stripe nor the chip on the Card can be read for any reason.

Note **Regional rule variations on this topic appear in chapter 17, "Asia/Pacific Region," and chapter 22, "United States Region," of this rulebook.**

7.7.3 PIN Entry Device

PIN entry devices must:

a. have a numeric keyboard to enable the entry of PINs;

b. have an 'enter key' function, in order to indicate the completion of the entry of a variable length PIN;

c. accept PINs having four (4) to six (6) numeric characters. Note: The Organization strongly recommends that PINs up to twelve (12) characters be supported.

Note **Regional rule variations on this topic appears in chapter 18, "Canada Region," and chapter 22, "United States Region," of this rulebook.**

7.7.4 Function Keys

It is recommended that a "cancel" function is provided in order to cancel a Transaction if an error is made, or if the Cardholder wishes to stop the Transaction before it is transmitted for authorization.

If an Acquirer allows for the cancellation of Transactions, a reversal must be sent for any Transaction that was canceled after it was authorized.

If the 'cancel' function is not supported, the POS Terminal or Terminal must be capable of clearing all previous information when reaching the time-out limitation, in order to be available for a new Transaction.

Two function keys are recommended. Their meaning should be understandable to Cardholders who do not speak the local language. The preferred color-coding and labeling for the different keys are provided below. If significant deviations from these preferred colors and labels are implemented, the Cardholder guidance information should contain appropriate descriptions.

a. The first key is used to restart the process of PIN entry or entry of the Transaction amount. The preferred color is yellow, and the preferred label is "CORR" or "Cancel."

b. If the optional function to terminate a Transaction is implemented, the corresponding key should be red, and the preferred label is "STOP" or "CANCEL."

Note **A regional rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

7.7.5 POS Terminal and Terminal Responses

POS Terminals and Terminals must be able to display or print the response required in the applicable technical specifications.

The Acquirer or the Merchant, as applicable, must provide an appropriate message to the Cardholder whenever the attempted Transaction is rejected. When a specific reason for the rejection cannot be provided, the message must refer the Cardholder to the Issuer.

7.7.6 Balance Inquiry

All POS Terminals and Terminals that currently offer a balance inquiry transaction to cardholders of Competing EFT POS Networks and competing networks must offer the same balance inquiry functionality to Cardholders.

Note **A regional rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

Note **An additional regional rule on this topic appears in chapter 22, "United States Region," of this rulebook.**

7.7.7 Card Authentication—Europe Region Only

Note **Regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.8 Hybrid POS Terminal and Hybrid Terminal Requirements

In addition to the requirements listed in section 7.7, all hybrid POS Terminals and hybrid Terminals must:

a. read required data from the chip when present in Chip Cards, and either transmit or process, as appropriate, all required data for authorization processing;

b. perform the Transaction using the EMV chip;

c. be capable of performing fallback procedures when the Transaction cannot be completed using chip technology because of a technical failure;

d. comply with the acceptance requirements set forth in the chip technical specifications, as published from time to time by the Organization;

e. be type-approved by the Organization before they accept Chip Cards;

f. request a cryptogram for all chip-read Transactions; if approved, transmit a transaction certificate and related data;

g. support full use of the multi-application capabilities of Chip Cards as follows:

   1. maintain a complete list of all application identifiers (AIDs) for all products they accept;

   2. receive and retain updates of AIDs for all products they accept;

   3. attempt to match all AIDs contained in the hybrid POS Terminal or hybrid Terminal with those on any EMV-compliant Chip Card used;

   4. display all matching application labels or preferred names to the Cardholder, except for those applications where a compatible product or application is permitted to take priority under the Rules;

   5. allow the Cardholder to select the application to be used when multiple matching applications exist, except where a compatible product or application is permitted to take priority under the Rules. (See '4' above);

6. provide the Cardholder the option of approving or canceling the Transaction, before the goods are dispensed, or the services performed.

Hybrid POS Terminals and hybrid Terminals that read and process EMV-compliant payment applications must read and process EMV-compliant Maestro payment applications, whenever an EMV-compliant Card is presented.

Note **An additional regional rule on this topic appears in chapter 19, "Europe Region," of this rulebook.**

7.8.1 Chip Liability Shift—Europe Region Only

Note **Regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.9 Additional Requirements for POS Terminals

In addition to the requirements listed in section 7.7:

a. each Merchant is responsible for the maintenance arrangements of its POS Terminals, unless the Acquirer undertakes this function; and

b. at POS Terminals that support both signature and PIN verification methods, the Cardholder must always be identified by a PIN. These POS Terminals must display a message stating that a PIN must be provided.

Note **An additional regional rule on this topic appears in chapter 17, "Asia/Pacific Region," and chapter 22, "United States Region," of this rulebook.**

7.9.1 Additional Requirements for Hybrid POS Terminals

In addition to the requirements listed in sections 7.7 POS Terminal and Terminal Requirements, 7.8 Hybrid POS Terminal and Hybrid Terminal Requirements, and 7.9 Additional Requirements for POS Terminals, hybrid POS Terminals must:

a. support both online and offline PIN as the CVM. On a country-by-country basis, the Organization may permit Acquirers to, at a minimum, support offline PIN as the CVM.

b. perform the following risk management functions: floor limit and Card velocity checking using the floor limits and parameters provided by the Organization. Where the Chip Card's maximum Transaction amount differs from the POS Terminal's floor limit, the lower amount governs;

Hybrid POS Terminals that connect to a full grade acquiring network must support online mutual authentication (OMA) and script processing.

Hybrid POS Terminals may provide a Transaction certificate in the clearing message, at the Acquirer's option.

Hybrid POS Terminals are not required to support offline Transaction processing. However, any hybrid POS Terminals that support offline Transaction processing must identify all offline Transactions as such to the Issuer when submitting the Transactions.

Note **An additional regional rule on this topic appears in chapter 19, "Europe Region," of this rulebook.**

7.12 POI Terminal Transaction Log

A POI Terminal Transaction log must be maintained.

The log must include, at a minimum, the same information provided on the Cardholder receipt, including the Card sequence number, if present. The log must include the full PAN, unless otherwise supported by supplementary reported data.

The log whether paper, fiche, or an online authorization file that may be available for research purposes at the Acquirer's site, must not include the PIN or any discretionary data from the Card's magnetic stripe or chip. Only the data necessary for research should be recorded. An Issuer may request a copy of this information.

The POI Terminal must not electronically record a Card's full magnetic stripe or chip data for the purpose of allowing or enabling subsequent authorization request.

The only exception to this rule is for Merchant-approved Transactions, acquired at POS Terminals, which subsequently have been declined by the Issuer. The Merchant may resubmit the Transaction for a period up to thirteen (13) calendar days after the Transaction date. In these circumstances, the required data may be logged until either the Transaction is authorized or the end of the thirteen (13)-day period, whichever occurs first.

When an attempted Transaction is rejected, an indication or reason for the rejection must be included on the Terminal Transaction log.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," and chapter 22, "United States Region," of this rulebook.**

7.13 Requirements for Transaction Receipts

For every completed authorized Transaction, a receipt must be made available to the Cardholder either automatically or upon the Cardholder's request.

For every completed authorized electronic commerce Transaction, a receipt page must be displayed after the Cardholder confirms a purchase. The display of the receipt on the screen must be printable.

If technically feasible, PIN-Based In-Branch Terminals must provide a Transaction receipt to the Cardholder either automatically or upon the Cardholder's request.

Discretionary data from the magnetic stripe or chip must not be printed on the receipt.

A balance inquiry, where offered, must make available (or optionally display) to the Cardholder, a receipt containing account balance information as specified in the applicable technical specifications.

If a Transaction receipt is produced following an unsuccessful Transaction attempt, the receipt must contain the response or failure reason, in addition to all other required information as specified in this section.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.13.1 Receipt Contents for POS Terminals

The contents of the receipt must be in accordance with the following minimum requirements:

a. Transaction amount (in a dual currency environment, the Transaction currency must be identified on the receipt; in all other environments, the Transaction currency symbol is recommended);

b. Transaction date;

c. Transaction type;

d. Account type selected (if supported);

e. primary account number (PAN)—(The PAN must be truncated as specified below);

f. POS Terminal number and/or location (retailer name and/or identification);

g. trace number;

h. Transaction time;

i. Transaction result; and

j. any other information required under applicable laws, Rules, and the regulations, policies, and technical specifications of the Organization.

If a receipt printer fails, a manual receipt may be substituted. The receipt must conform to the receipt requirements described above, with the exception of the trace number.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

7.13.2 Receipt Contents for Terminals

The contents of the receipt must be in accordance with the following minimum requirements:

a. identification of the Acquirer (e.g. institution name, logotype);

b. local time;

c. local date;

d. Transaction amount (in a dual currency environment, the Transaction currency must be identified on the receipt; in all other environments, the Transaction currency symbol is recommended);

e. Terminal identification;

f. Card identification (PAN must be truncated as specified below)

g. Transaction type;

h. Transaction sequence number; and

i. a statement that the Transaction was for the purchase of goods or services (Merchandise Transaction only).

Acquirers are encouraged to offer a printed receipt only as a Cardholder-activated option.

It is recommended that receipts be printed in English.

Terminals must clearly describe, by receipt, screen information, or both, the action taken by the Issuer and INFs in response to a Cardholder's request, (approved or rejected).

It is recommended that INFs and Terminals interpret the denial codes sent by the Issuer in accordance with appendix F, "Signage, Screen, and Receipt Text Standards."

7.13.3 Receipt Contents for Electronic Commerce Transactions

The contents of any e-mail acknowledgement of the Cardholder's order must be in compliance with all other requirements for a Transaction receipt, as set forth in this section.

7.13.4 Balance Inquiry Display

For balance inquiries, Terminals must display as part of the screen information, or must print on the receipt the currency symbol of the local currency or three (3)-character alpha ISO country code, in which the balance amount is given, beside each balance inquiry amount.

Note **A regional rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

7.13.5 PAN Truncation Requirements

7.13.5.1 POS Terminals

Subject to applicable laws, Rules and regulations, the receipt at unattended POS Terminals must reflect a minimum of four and a maximum of twelve digits of the PAN. At least four (4) digits must be truncated.

It is strongly recommended that Cardholder receipts generated by attended and unattended POS Terminals reflect only the last four (4) digits of the PAN, replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as "x", "*", or "#."

The Cardholder receipt generated by newly installed, replaced or relocated POS Terminals deployed on or after 1 April 2005, whether attended or unattended, must reflect only the last four (4) digits of the PAN, replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as "x", "*", or "#".

7.13.5.2 Terminals

One (1) of the following options must be used:

a. print the PAN on the receipt but truncate a minimum of any four (4) digits of the PAN. The Organization strongly recommends that all truncated digits be replaced with fill characters that are neither blank spaces nor numeric characters, such as "x", "*", or "#"; or

b. print the PAN on the receipt but render a minimum of any four (4) digits of the PAN indeterminable by any Organization approved method.

The Organization strongly recommends that the receipt reflect only the last four (4) digits of the PAN, replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as "x", "*", or "#."

The receipt generated by newly installed, replaced or relocated Terminals deployed on or after 1 April 2005, must reflect only the last four (4) digits of the PAN, replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as "x", "*", or "#."

7.13.6 Chip Transactions

In addition to the minimum data elements, receipts related to chip Transactions must contain the application label and may, at the Acquirer's discretion, additionally contain the Transaction certificate and related data.

7.14 POS Terminal and Terminal Availability

Each Acquirer must take all reasonable actions to ensure that all POS Terminals and Terminals are available for use by Cardholders during normal business hours.

"Normal business hours" are those hours customarily observed in the location at which the Card is being used.

7.17 Return of Cards—POS Transactions Only

Merchants may return a Card inadvertently left at their Merchant location, to the Cardholder, until the close of the following Merchant business day. Merchants may only return a Card if the Cardholder provides positive identification.

A Card not claimed by the Cardholder by the close of the following Merchant business day must be processed in accordance with the applicable merchant agreement.

8.5 Triple DES Migration Processing Plan

POS Terminals are required to use Triple DES, minimum double key length (hereafter referred to as "Triple DES"), in accordance with the following implementation schedule set out below:

a. Members, at their option, may use "Triple DES."

b. All newly installed POS Terminals, including replacements, must be "Triple DES" capable.

c. All Members and processor host systems must support "Triple DES".

d. It is strongly recommended that all POS Terminals be "Triple DES" compliant and be chip capable.

e. Effective 1 April 2007, it is strongly recommended that all POS Terminals read and act on extended service codes.

ATMs are required to use Triple DES, double key length (hereafter referred to as "Triple DES"), in accordance with the following implementation schedule set out below:

a. Members, at their option, may use "Triple DES."

b. All newly-installed ATMs, including replacements, must be "Triple DES" capable.

c. All Member and processor host systems must support "Triple DES."

d. All ATMs must be "Triple DES" compliant.

e. It is strongly recommended that all ATMs be chip capable.

Members may elect to use other key encryption methodologies between their POS Terminals, ATMs and their host. In such instances, the alternate methodology chosen must be evaluated as more secure than "Triple DES" and approved by the Organization before implementation. However, all Transactions routed to the Interchange System must be "Triple DES" compliant.

9.1 POS Transaction Types

9.1.2 Acquirer Online POS Transactions

9.1.2.1 Required Transactions

Acquirers and Merchants must ensure that each POS Terminal supports the electronic processing of the following online POS Transactions:

a. Purchase (from primary account or account selection from checking and savings account):

   Acquirers must ensure that purchases are initiated using a card reader and a PIN or, if the Organization has given a waiver, a signature to identify the Cardholder. Refer to chapter 7, "Acquiring," for additional 'card reader' information.

b. Reversal (this Transaction typically is sent as a result of an Acquirer-side technical problem or a 'cancel'):

   Acquirers must support reversals for the full amount of any authorized Transaction whenever the system is unable, because of technical problems, to communicate the authorization response to the POS Terminal.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," and chapter 20, "Latin America and the Caribbean Region," of this rulebook.**

Note **A regional rule variation on this topic appears in chapter 17, "Asia/Pacific Region," and chapter 22, "United States Region," of this rulebook.**

9.1.2.2 Optional Online POS Transactions

Acquirers and Merchants may offer, any or all of the following online Transactions, to the extent permitted by law, regulations, or both, and as permitted within a Region:

a. Balance inquiry:

   Acquirers must ensure that balance inquiries, if supported, are initiated using a PIN and a Card.

b. Purchase variations as follows:

   1. Scrip:

      POS Terminals may dispense scrip to perform purchases.

      Scrip may not be redeemed solely for cash.

      All unredeemed scrip must be reversed within four (4) calendar days of issuance. An Acquirer may establish a shorter time period at its option.

      All scrip Transactions must be PIN-based Transactions and authorized and settled as retail Transactions.

   2. Purchase with cash back.

      Acquirers and Merchants that choose to provide the purchase with cash back Transaction must establish an education program for retail employee staff including, but not limited to, POS terminal operators.

      Purchase with cash back Transactions must occur in a card-present environment and must be verified using the cardholder PIN (except for purchase with cash back Transactions that occur in Maestro-approved signature variance countries.)

      For all PIN-verified purchase with cash back Transactions, the Acquirer and Merchant should establish a maximum cash back amount. For all signature-verified purchase with cash back Transactions, a maximum cash back amount of USD 100 (or its local currency equivalent) must be observed.

      Acquirers and Merchants must ensure that cash is provided only when combined with a purchase Transaction. The purchase, cash back, and total Transaction components of the purchase with cash back Transaction must be in the same currency.

Acquirers must submit authorization and clearing records that include a purchase with cash back Transaction identifier and two amount fields. The first amount field must set forth the total Transaction amount. The second amount field must set forth the amount of cash back included in the total Transaction amount. A maximum cash back amount of USD 100 (or local currency equivalent) applies for all cross-border purchases with cash back Transactions.

The Acquirer and Merchant may prompt the Cardholder to use the purchase with cash back Transaction.

Note **An additional regional rule on this topic appears in chapter 22, "United States Region," of this rulebook.**

3. Merchant-approved purchase:

   Merchant-approved Transactions may be processed by the Acquirer, providing specific written approval to process such Transactions has been given by the applicable Maestro Regional Licensor. The Maestro Regional Licensor must verify that the Acquirer strictly adheres to security requirements.

   Acquirers may elect to accept Merchant-approved Transactions, only when the POS Terminal cannot receive an authorization for a Transaction because of technical difficulties between the Acquirer and the Interchange System, or the Interchange System and the Issuer.

   These Transactions may be accomplished only by using electronic store and forward, and when the Card is read by a POS Terminal.

   Each Acquirer must forward all stored Transactions as soon as the technical problem has been resolved.

   Issuers must treat all such Merchant-approved Transactions as financial request messages. The Acquirer bears all liability for Merchant-approved Transactions, which when forwarded, are declined by the Issuer.

   If the Issuer is unavailable to authorize or decline such a Merchant-approved Transaction at the time of presentment, the Interchange System will indicate this, and return the Transaction to the Acquirer. These returned Transactions may be submitted by the Acquirer to the Interchange System every thirty (30) minutes, until a response is received from, or on behalf of the Issuer.

   Merchant-approved Transactions will settle only upon positive authorization by the Issuer.

If a Merchant-approved Transaction is subsequently declined by the Issuer for insufficient funds, or because the Transaction exceeds withdrawal limits, the Acquirer may resubmit the Transaction once every twenty-four (24) hours for a period ending thirteen (13) calendar days after the Transaction date.

Issuers and Maestro Regional Licensors are not required to assist Acquirers in any attempt to collect on Merchant-approved Transactions.

4. Pre-authorization (or funds guarantee) and pre-authorization completion:

   Acquirers must ensure that pre-authorizations (in the physical environment) are initiated using a card reader, and a PIN or signature for Cardholder identification. Refer to chapter 7, "Acquiring," for additional "card reader" information.

   Issuers must accept all pre-authorization completions provided the actual amount of the completion is less than or equal to the amount approved in the pre-authorization. Use of the PIN or signature and the use of the card reader are not required in the pre-authorization completion.

   If the Issuer does not receive a pre-authorization completion within twenty (20) minutes of the pre-authorization, the pre-authorization approval is void, except as provided for under Merchant-approved Transaction processing requirements, which are described in this section.

   Acquirers are not liable for pre-authorization completions that occurred within two (2) hours of the initial Transaction that were stored and forwarded because of technical problems between the Acquirer and the Interchange System, or the Interchange System and the Issuer.

5. Correction:

   Following the authorization of a Transaction, corrections may be used to correct a Merchant or Cardholder error. Corrections must be initiated by or on behalf of the Cardholder by use of a PIN or signature, and electronic reading of the Card in a card reader.

   The Acquirer assumes the risk for this Transaction and the interchange fee is returned to the Acquirer from the Issuer.

6. Cancel.

7. Refund.

8. Payment Transaction:

   A Payment Transaction does not reverse a prior POS Transaction.

Each Acquirer that has an agreement with a Merchant to perform electronic commerce Transactions must additionally support the Account in Good Standing, non-financial Transaction.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," and chapter 20, "Latin America and the Caribbean Region," of this rulebook.**

Note **A regional rule variation on this topic appears in chapter 17, "Asia/Pacific Region," and chapter 22, "United States Region," of this rulebook.**

9.1.4 Acquirer Offline POS Transactions

Each Merchant and Acquirer may offer at each hybrid POS Terminal participating in the Organization, offline processing of the following chip-read Transactions:

a. purchase from primary Account

b. purchase from checking Account

c. purchase from savings Account

d. refund

The Acquirer may clear offline Chip Card Transactions by transmitting an online Financial Advice/0220 message containing required data, or may transmit required data as part of a batch notification, for each Transaction.

Note **A regional rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

9.1.5 Offline Processing—POS Transactions

If a Transaction that may be processed offline cannot be so processed for any reason except CAM failure, the POS Terminal must process the Transaction online. However, if the POS Terminal is not capable of going online, the Transaction must be declined.

If there is CAM failure and online processing is not possible, or if the POS Terminal finds that the presented Chip Card is on the Emergency BIN List, the Transaction must be declined. Refer to chapter 7, "Acquiring," for hybrid POS Terminal CAM policy.

9.2 Terminal Transaction Types

9.2.2 Acquirer Requirements

Terminals must offer cash withdrawals from an Account. (Refer to chapter 6, "Issuing" subsection 6.1.3 for additional information).

Terminals must not dispense scrip.

Acquirers are prohibited from automatically generating online reversals for the full or partial amount of any authorized cash disbursement Transaction when a Terminal indicates that such Transaction was not completed because the Cardholder failed to collect some or all of the cash dispensed.

All Terminals that offer balance inquiry functionality to cardholders of competing networks must offer the same balance inquiry functionality to Cardholders.

During Account selection, all Terminals must include the word "Savings" when offering a cash withdrawal or transfer from a savings account; and the word "Checking" or "Chequing" when offering a cash withdrawal or transfer from a checking account.

Note **Additional regional rules and rule variations on this topic appear in chapter 18, "Canada Region," and chapter 19, "Europe Region," of this rulebook.**

9.2.2.1 Acquirer—Optional Transactions

Terminals may offer the purchase of Merchandise by Cards from no account specified, to the extent permitted by law, regulations, or both, and as permitted within a Region.

Note **An additional regional rule on this topic appears in chapter 18, "Canada Region," and a rule variation on this topic appears in chapter 19, "Europe Region," of this rulebook.**

9.2.3 Terminal Edit Specifications—Europe Region Only

Note **Regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

9.3 Special Transaction Types

Special Transaction processing requirements apply to the types of Transactions listed in this section.

They must be processed with the specific merchant category codes (MCC) indicated.

9.3.1 Processing Requirements—POS Special Transaction Types

Cardholder entered PINs are required for the POS Transaction types outlined in this subsection that are conducted in the face-to-face environment. MasterCard SecureCode must be utilized as the CVM for quasi cash and gambling Transactions conducted through the Internet.

Waivers granted regarding the acceptance of Transactions using signature rather than PIN are not applicable to the following Transaction types:

a. Money Transfer (MCC 4829—Merchant)

   A Transaction in which funds are delivered or made available to person(s), other than the Cardholder, at a location other than the location at which the money transfer is initiated. Any fee charged for this Transaction and included in the total Transaction amount must be clearly disclosed to the Cardholder in advance of completing the Transaction. Members must include the identity and location of the money transfer agent that accepts the Card and effects the Transaction in the card descriptor record as the site where the Transaction was effected.

b. Money Transfer (MCC 6534—Member Financial Institution)

   A Transaction in which funds are delivered or made available to person(s) other than the Cardholder initiating the money transfer, at a location other than the Member location at which the money transfer is initiated. Any fee charged and included in the total Transaction amount must be clearly disclosed to the Cardholder in advance of completing the Transaction.

c. Quasi Cash (MCC 6050—Member Financial Institution)

A Transaction in which a Card is used to purchase travelers checks, foreign currency, money orders, precious metals, or savings bonds at a Member financial institution. This MCC also identifies Transactions in which a Member financial institution accepts a Card in direct payment of an existing debt, such as a private label card or vehicle loan. Any fee charged and included in the total Transaction amount must be clearly disclosed to the Cardholder in advance of completing the Transaction.

This MCC must be used for non-face-to-face transactions, such as those facilitated through the Internet.

d. Quasi Cash (MCC 6051—Merchant)

A Transaction in which a Card is used to purchase travelers checks, foreign currency, or money orders, or a Card is used to open a deposit account, at a location other than a Member financial institution. This MCC also identifies Transaction in which a Merchant accepts a Card for payment of an existing debt, such as a private label card or vehicle loan. Any fee charged and included in the total Transaction amount must be clearly disclosed to the Cardholder in advance of completing the Transaction.

For the face-to-face purchase of foreign currency, money orders, or travelers checks at a Member financial institution, use MCC 6010.

e. Gambling Transactions (MCC 7995)

Any Transaction, other than an ATM or PIN-Based In-Branch Terminal Transaction, which involves placing a wager, purchasing a lottery ticket, in-flight commerce gaming, or purchasing gambling chips or other instruments redeemable for cash, goods or services in conjunction with gambling activities. Any fee charged in connection with such gaming Transactions, must be clearly disclosed to the Cardholder in advance of completing the Transaction, and included in the total Transaction amount. Such a fee may not be charged for in-flight commerce gaming transactions.

f. Truck Stop Transactions (MCC 7511)

Any Transaction, other than an ATM or PIN-Based In-Branch Terminal transaction that is conducted at fuel desks of truck stops, weigh stations, public scales, or ports of entry. Any fee charged in connection with such Transactions, must be clearly disclosed to the Cardholder in advance of completing the Transaction, and included in the total Transaction amount. Truck stop Transactions must be conducted face-to-face.

9.3.2 Processing Requirements—Electronic Commerce and Payment Transactions (Other Special Transactions)

Cardholder entered PINs are not required for electronic commerce or Payment Transactions outlined in this subsection.

The Card expiration date is optional for the following Transaction types:

a. Remote Stored Value Load (MCC 6529—Member Financial Institution)

   A non–face-to-face sale (excluding ATM transactions) of electronic value or the funding of a deposit account at a Member financial institution by means of a Card. Any fee charged and included in the total Transaction amount must be clearly disclosed to the Cardholder in advance of completing the Transaction.

b. Remote Stored Value Load (MCC 6530—Merchant)

   A non–face-to-face sale (excluding ATM transactions) of electronic value or the funding of a deposit account at a location other than a Member financial institution by means of a Card. Any fee charged and included in the total Transaction amount must be clearly disclosed to the Cardholder in advance of completing the Transaction.

c. Payment Service Provider (MCC 6531—Money Transfer for a Purchase)

   Use of this MCC is restricted to Members and Merchants that the Organization has registered as Payment Service Providers. This MCC identifies a Transaction in which the Payment Service Provider accepts funds from a Cardholder for the sole purpose of transferring the funds to a seller of goods or services purchased by the Cardholder. The Payment Service Provider is not itself the seller of goods or services, but rather acts as the intermediary between the Cardholder and the seller. This MCC requires that Payment Service Providers assume responsibility for the quality and delivery of the goods or services purchased by the Cardholder.

   Use a TCC of R for face-to-face transactions and a TCC of T for non–face-to-face transactions.

d. Payment Service Provider (MCC 6532—Member Financial Institution)

   Use of this MCC is restricted to Members that the Organization has registered as Payment Service Providers. This MCC may be used only to identify Payment Transactions. A Payment Transaction allows Cardholders to receive funds via a posting to an Account held or overdraft credit lines extended by their Issuer. A Payment Transaction does not reverse a previous purchase Transaction and must be authorized by the Issuer.

e. Payment Service Provider (MCC 6533—Merchant)

Use of this MCC is restricted to Merchants that the Organization has registered as Payment Service Providers for the purpose of performing Payment Transactions. This MCC may be used only to identify Payment Transactions. A Payment Transaction allows Cardholders to receive funds via a posting to an Account accessed by a Card extended by their Issuer. A Payment Transaction does not reverse a previous purchase Transaction and must be authorized by the Issuer.

A Payment Transaction (MCC 6532—Member Financial Institution or 6533—Merchant) must be effected in a way that does not conflict with Cardholder agreements or instructions.

9.4 Processing Requirements

The following requirements apply only to electronic functions performed by POI Terminals, Merchant processors or Acquirer Processors, and do not apply to manual functions performed at the POS:

a. Transactions initiated with a Card may not be declined due to BIN/IIN validation by POI Terminals, Merchant processors or Acquirer Processors if the BIN/IIN of such a Card begins with:

1. "50";
2. "56" through and including "58"; or
3. "60" through and including "69."

b. Transactions initiated with a Card may not be declined by POI Terminals, Merchant processors or Acquirer Processors as a result of edits or validations performed on the following data elements:

1. PAN length;
2. expiration date;
3. service code;
4. discretionary data; or
5. check digit.

Acquirers and Acquirer Processors are discouraged from editing the transposition check digit. See appendix B, "Technical Specifications."

9.4.1 Track 1 Processing

Acquirers and Acquirer Processors must not perform tests or edits on track 1 for the purpose of disqualifying Cards from eligibility for processing within the Organization.

9.4.2 PAN Processing

Acquirers and Acquirer Processors must accept all PAN lengths in Cards when such PAN lengths are in compliance with chapter 6, "Issuing," of the Rules.

Acquirers and Acquirer Processors must accept all valid major industry identifier numbers and IINs in Cards when such major industry identifier numbers and IINs are in compliance with chapter 6, "Issuing," of the Rules.

9.4.3 Card Data Processing

Acquirers and Acquirer Processors must accept all Card expiration and effective dates, as well as all Chip Card application effective dates, when dates are in compliance with chapter 6, "Issuing," of the Rules. Note: It is strongly recommended that these fields not be edited.

Acquirers and Acquirer Processors are not required to act on the extended service codes at this time unless a value of 2 is present in position 1 for a Maestro payment application. The hybrid POS Terminal and hybrid Terminal must first attempt to process the Transaction as a chip Transaction. For additional information, refer to the MasterCard *Authorization System Manual.*

Acquirers and Acquirer Processors must accept all Card service code values, when such service code values are in compliance with chapter 6, "Issuing," of the Rules.

Acquirers and Acquirer Processors must accept any character(s) in the discretionary data portion of Cards, when such discretionary data character(s) is in compliance with chapter 6, "Issuing," of the Rules.

9.4.4 Chip Card Processing

Acquirers must operate hybrid POS Terminals and Terminals in compliance with the technical specifications. Chip Transactions must be processed in accordance with the chip technical specifications as published from time to time by the Organization.

All Chip Card Transactions performed at hybrid Terminals must be authorized online to the Issuer, whether the magnetic stripe or chip is used to initiate the Transaction. Transactions performed at hybrid Terminals may not be authorized offline by means of the chip in the event that an online authorization can not be completed for technical reasons.

All hybrid POS Terminals and Terminals must perform fallback procedures, unless prohibited by the Maestro Regional Licensor.

9.5 Processing Electronic Commerce Transactions

Issuers who permit their Cardholders to perform electronic commerce Transactions must be capable of processing these Transactions when presented by an Acquirer.

Acquirers must properly identify an electronic commerce Transaction as specified in the *MasterCard SecureCode Member Enrollment and Implementation Guide*.

The merchant category code (MCC) of the underlying commercial activity of the Merchant must be used. MCCs for other modes of delivery (such as mail order) must not be used.

All electronic commerce Transactions have a zero floor limit and must be authorized by the Issuer or its agent. Acquirers must support the standard Issuer authorization response messages as specified in the technical specifications of the Organization.

The Merchant must accept and send unaltered, the thirteen (13) to nineteen (19)-digit PAN and the four (4) digits displayed in the expiration date field, together with data from the 'hidden form fields' into the Interchange System. Transactions may not be declined by the Merchant or Acquirer, as a result of edits or validations performed on the BIN/IIN or expiration date.

9.5.1 Cardholder Verification Method (CVM) Policy for Electronic Commerce Transactions

It is the Issuers' responsibility to decide which CVMs are acceptable for the completion of electronic commerce Transactions.

9.6 Authorizations

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

9.6.1 Cash Withdrawal Transactions

Cash withdrawal Transactions must be either approved or denied for the amount requested. No "less than requested" authorizations will be permitted.

9.6.2 Terminal Transaction Routing

Each Maestro Regional Licensor must ensure that all interregional Transactions are sent to the Interchange System except:

a. when the Issuer of the Card and the Acquirer of the Terminal are both majority-owned and operated by the same global bank or global bank holding company and who:

   1. are both Issuers; or

   2. use a proprietary brand or identifier of the global bank or global bank holding company to identify the Card and Terminal to the Cardholder;

b. when a sharing agreement exists between the Issuer and the Acquirer, and such agreement was executed before 31 December 1996, and when another common brand is utilized to identify the Card and Terminal to the Cardholder;

c. when the Transaction is a proprietary transaction.

Acquirers may default route to the Interchange System any Transaction not belonging to their proprietary network. It will be the responsibility of the Interchange System to determine whether or not the Transaction is being performed by a Cardholder.

Acquirers who do not default route must update their financial institution table (FIT) within six (6) calendar days of being informed of a change by the Interchange System. Acquirers who do not default route to the Interchange System must use the FIT for routing before default routing to any competing network.

Any Transaction generated by an application identified as an Interchange System AID scheme must be routed through the Interchange System, or as otherwise approved by the Organization.

Note **Additional regional rules on this topic appear in chapter 18, "Canada Region," chapter 20, "Latin America and the Caribbean Region," and chapter 22, "United States Region," of this rulebook.**

9.6.3 Location Information Requirements

9.6.3.1 Transaction Location

At the time of each Transaction, the Acquirer must transmit, in the field(s) specified in the applicable technical specifications, the generally accepted location, city, and country of the POS Terminal or Terminal substantially the same as it appears on any POS Terminal or Terminal receipt provided.

9.6.3.2 Terminal Location Reporting

Principal Members are required to provide the Organization with current and accurate information regarding its and its sponsored Members' Terminals by updating quarterly the ATM Directory located on MasterCard OnLine®.

9.6.4 Authorization Response Time

9.6.4.1 Issuer Response Time Requirements

An Issuer must respond to an ATM authorization request within twenty (20) seconds. If a response is not received within twenty (20) seconds, a time-out message will be generated to the Acquirer or the Transaction will be authorized using Stand-In Processing Service.

An Issuer must respond to a POS authorization request within ten (10) seconds. If a response is not received within ten (10) seconds, a time-out message will be generated to the Acquirer or the Transaction will be authorized using the Stand-In Processing Service.

Refer to section 9.7 of the Rules for additional information regarding Stand-In Processing Service.

Note **Additional regional rules on this topic appear in chapter 22, "United States Region," of this rulebook.**

9.6.4.2 Acquirer Response Time Requirements

Each Acquirer must wait a minimum of thirty (30) seconds for a Transaction response, before timing out a Transaction and forwarding a timeout message to the Issuer, unless a different timer value is agreed to by the Acquirer and the Organization.

Each Acquirer must ensure that its POS Terminals and Terminals adhere to the minimum timeout requirements.

Refer to the applicable technical specifications for further information about authorization response times.

Note **Regional rule variations on this topic appear in chapter 22, "United States Region," of this rulebook.**

9.6.5 Offline Chip Authorizations—Europe Region Only

Note **Regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

9.7 Performance Standards

Issuers and Acquirers that fail to meet performance standards may be subject to noncompliance assessments as set forth in subsection 9.7.3 below or may be mandated to implement the Stand-In Processing Service.

Note **Additional regional rules on this topic appear in chapter 19, "Europe Region," of this rulebook.**

9.7.2 Acquirer Terminal Standards

9.7.2.1 Acquirer Failure Rate

An Acquirer failure rate that exceeds two percent (2%) for POS or ATM Transactions for two (2) consecutive months is substandard. Terminal processing standards will not apply to Processors until:

a. after the fourth calendar month of such Processor's operation; or

b. upon such Processor's first processing five thousand (5,000) POS or ATM Transactions in a calendar month;

whichever occurs first.

The Acquirer failure rate is calculated based on the monthly volumes of POS or ATM Transactions processed through each Acquirer connection to the Interchange System and is calculated according to the formula below:

The sum of the following ISO 8583 response codes:

a. 13 invalid amount

b. 30 format error

Divided by the total number of POS and ATM Transactions processed through the Acquirer connection to the Interchange System.

Rules Applicable Only to the Asia/Pacific Region

Set forth below are the Rule variations to the *Maestro® Global Rules* and additional rules for the Asia/Pacific Region. These rules are excerpted from chapter 17, "Asia/Pacific Region," of the *Maestro Global Rules*. These rules apply only to the Asia/Pacific region.

7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only

In addition to the rules in chapter 7, "Acquiring," section 7.2 in part 1 of this rulebook, the following applies:

a. ensure that a Merchant requests online authorization for any Transaction conducted with a Card on which the expiration date embossed on the face of the Card has passed.

7.2.5 Refinancing of Previously Existing Debt and/or Payment of Bad Debts

Transactions representing the refinancing of an existing obligation of a Cardholder, including, but not limited to obligations:

a. previously owed to the Merchant; or

b. arising from the dishonor of a Cardholder's personal cheque, or any Transaction(s) representing the collection of any other pre-existing indebtedness,

are not permitted.

7.7 POS Terminal and Terminal Requirements

7.7.2 Manual Key-Entry of PAN

The following replaces chapter 7, "Acquiring," subsection 7.7.2 in part 1 of this rulebook:

If the POS Terminal's magnetic stripe reader is disabled or the stripe on the Card is unreadable, manual entry of the Card PAN is supported as a fall back procedure. The Cardholder and the Card must be physically present at the location and time of the Transaction, and the Cardholder must enter a PIN to effect the Transaction. Issuers may deny these Transactions as a result of missing data.

7.9 Additional Requirements for POS Terminals

In addition to the rules in chapter 7, "Acquiring," section 7.9 in part 1 of this rulebook, the following applies:

a. POS Terminals must contain keyboards that assign letter-number combinations as described in section 7.10 in part 1 of this rulebook.

7.22 Return Merchandise Adjustments, Credits, and Other Specific Terms of a Transaction

With proper disclosure at the time of any Transaction, a Merchant:

a. is not obliged to accept merchandise in return or exchange or to issue refunds to Cardholders;

b. may only accept merchandise in immediate exchange for similar merchandise of a price equal to the amount of the original Transaction;

c. may accept merchandise in return and deliver to the Cardholder a credit slip for the value of the merchandise returned, which may be used only in the Merchant's place(s) of business;

d. if permitted by applicable law, may stipulate special circumstances agreed to by the Cardholder, e.g., late delivery charges, insurance charges; or

e. may cause the Transaction to be completed in respect of Transactions involving the delayed delivery of goods or services.

For the purposes of this section, proper disclosure is deemed to have been definitely given at the time of the Transaction if the following or similar wording appeared legibly on all copies of the Transaction receipt or on an invoice issued at the time of the sale prior to the receipt being presented to the Cardholder (lack of this wording does not necessarily mean proper disclosure has not been given):

as related to paragraph (a) — "NO REFUND" as related to paragraph (b) — "EXCHANGE ONLY" as related to paragraph (c) — "IN-STORE CREDIT ONLY" as related to paragraph (d) — (ANY SPECIAL TERMS)

If proper disclosure is not made at the time of the Transaction and any merchandise is accepted for return or any services are terminated or cancelled, or any price adjustment is allowed by the Merchant, the Merchant is allowed to make a cash refund to the Cardholder, or the Merchant must process an on-line credit Transaction to the Issuer, and provide the Cardholder a credit receipt evidencing such refund or adjustment. The Merchant must sign and date each credit receipt and must include thereon a brief identification of the

merchandise returned, services cancelled or adjustment made and the amount of the credit in sufficient detail to identify the Transaction.

13.8 Pre-authorized Transactions

The following replaces chapter 13, "Liabilities and Indemnification," paragraph 1 of section 13.7 in part 1 of this rulebook:

An Issuer is liable for any Transaction, for which the Acquirer obtained a pre-authorization, and, which the Acquirer stored and forwarded to the Issuer within twenty (20) minutes of the pre-authorization.

Rules Applicable Only to the Canada Region

Set forth below are the Rule variations to the *Maestro® Global Rules* and additional rules for the Canada region. These rules are excerpted from chapter 18, "Canada Region," of the *Maestro Global Rules*. These rules apply only to the Canada region.

7.7 POS Terminal and Terminal Requirements

7.7.3 PIN Entry Device

The following replaces chapter 7, "Acquiring," subsection 7.7.3 c. in part 1 of this rulebook:

c. be capable of allowing entry of PINs having from four (4) to twelve (12) characters.

9.2 Terminal Transaction Types

9.2.2 Acquirer Requirements

In addition to the requirements of chapter 9, "Processing Requirements," subsection 9.2.2 in part 1 of this rulebook, the following apply:

Terminals must offer the following Transactions to the extent permitted by law, regulation, or both.

a. cash withdrawal from a savings Account;

b. cash withdrawal from a checking (or chequing) Account;

c. cash advance from a credit card.

Terminals must offer the following Transaction(s) to the extent permitted by law, regulation, or both, if that Transaction(s) is offered to a Competing Network(s).

a. balance inquiry—checking (or chequing) Account;

b. balance inquiry—savings Account;

c. balance inquiry—credit card;

d. transfer from checking (or chequing) to savings Account;

e. transfer from savings to checking (or chequing) Account.

All Terminals that perform cash withdrawals not requiring account selection must convert those Transactions to withdrawal from no Account specified.

9.6 Authorizations

9.6.2 Terminal Transaction Routing

Whenever a Card issued in the Region is used at a Terminal in the Region and the only common brand on the Card and Terminal is a Service Mark:

a. the resulting Transaction must be routed to the Interchange System; or

b. the Issuer receiving such Transaction must:

   1. report such Transaction in accordance with the schedule and other requirements of chapter 15, "Fees," in part 1 of this rulebook; and

   2. pay a Brand Fee for such Transaction as required by chapter 15, "Fees, in part 1 of this rulebook,"

except when the Transaction was:

a. processed between a Principal Member (or its processor) and one of its Affiliate Members (or its processor), or

b. processed between two Affiliate Members (or their processors) sponsored into the Organization by the same Principal Member.

Note **The first paragraph of this subsection does not apply if the transaction is a proprietary transaction.**

Rules Applicable Only to the Europe Region

Set forth below are the Rule variations to the *Maestro® Global Rules* and additional rules for the Europe region. These rules are excerpted from chapter 19, "Europe Region," of the *Maestro Global Rules*. These rules apply only to the Europe region.

3.7 Record Retention

In addition to the rules in chapter 3, "Common Obligations," section 3.7 in part 1 of this rulebook, the following applies:

If a Transaction is disputed before the expiration of the minimum storage period, all records relevant to the Transaction must be stored until the dispute is finally resolved.

4.2 Use of the Service Marks

In addition to the rules in chapter 4, "Service Marks," section 4.2 in part 1 of this rulebook, the following apply:

a. Only Members who have a Maestro license, and Merchants from whom these Members acquire Transactions, may use the Service Marks. Refer to chapter 1, "Introduction and Participation Requirements," section 1.2.1 c) in part 1 of this rulebook, for the eligibility criteria applicable in the Europe Region.

b. Members must obtain approval from MasterCard Europe before placing the Service Marks on Cards, POS Terminals, Terminals, or any promotional material produced by Members themselves or Merchants.

c. When using the Service Marks, the Member must include a notice of the owner's rights to the Service Marks, and any other information that may be required.

d. In order to demonstrate compliance with the Rules, Members must, on MasterCard Europe's request, immediately provide copies of the following:

   1. items of their own displaying the Service Marks (for example, decals or other promotional material);
   2. items used by Member Service Providers;
   3. items used by Merchants with which the Member has agreements.

e. A third party, that is not the Member's MSP or Merchant, may only display the Service Marks if the Organization has given written authorization to do so.

4.4 Display of the Service Marks at POI Terminals

In addition to the rules in chapter 4, "Service Marks," section 4.4 in part 1 of this rulebook, the following apply:

The minimum size permitted for reproduction of the Service Marks on or near a POI Terminal is fifty (50) mm each in width. The width of the Service Marks should be measured from left edge to right edge of the blue background box.

The Service Marks must have equal prominence with international, regional, and bilateral marks displayed on the same POI Terminal.

The Service Marks must be shown in full-color according to the color specifications, provided by MasterCard Europe.

Display at POS Terminals

Upon request, Acquirers must make artwork or transparencies of advertising material that feature the Service Marks available to Merchants. Such material is available from MasterCard Europe.

Display at Terminals

The Service Marks must appear on or near the Terminal and must be applied in such a way that Cardholders can immediately recognize that the Terminal is associated with the Maestro brand.

Display of the Service Marks in Advertising

All advertising that makes reference to the Service Marks must be submitted to MasterCard Europe for approval before being released.

Merchants that wish to show they accept Cards as a means of payment in their own advertising do not need MasterCard Europe's permission to use the Service Marks, provided that:

a. the Service Marks do not occupy a prominent position (i.e. not more than ten percent (10%) of advertising space);

b. the Organization does not appear to endorse a product or service (see "Use of the Service Marks" in chapter 4, part 1 of this rulebook).

If the Merchant places its own advertising in the press or other media to show it accepts Cards as a means of payment, it may be required to supply its Acquirer with specimens of all materials bearing the Service Marks.

4.5 Protection of the Service Marks

In addition to the rules in chapter 4, "Service Marks," section 4.5 in part 1 of this rulebook, the following apply:

A Member must not register the Service Marks in its own name or in any owner's name.

A Member must not use or register or aid third parties in using or registering any trademark or tradename, which is confusingly similar to any of the Service Marks.

If MasterCard Europe finds that the activities of a Member, MSP, or sales agent are harmful to the Service Marks, the Member must ensure that such activities cease immediately.

A Member must notify MasterCard Europe immediately if it discovers that a third party:

a. is using the Service Marks without authorization;

b. is otherwise infringing the owner's rights regarding the Service Marks; or

c. has a conflicting claim to the Service Marks.

MasterCard Europe may require the Member to correspond with the third party on behalf of MasterCard Europe and in accordance with the instructions of MasterCard Europe.

The Member must take such measures as MasterCard Europe or the owner may require to assist it in any actions to register, perfect, maintain, or protect the owners' rights to the Service Marks. The Member may be required by MasterCard Europe or the owner to litigate in the Member's own name, on behalf of the owner, if the owner is legally prevented from litigating in its own name. All activities relating to such assistance will be decided upon and be under the control of MasterCard Europe or the owner. The owner will pay the Member's out-of-pocket expenses related to these activities.

5.1 Applicability of the Standards

In addition to the rules in chapter 5, "Special Issuer Programs," section 5.1 in part 1 of this rulebook, the following apply:

"Affinity Card Program" shall mean a card program that solicits individuals who share common interests, activities or membership in a specific organization. Many of these organizations (also know as "Affinity Groups") are non profit.

"Co-Branded Card Program" shall mean a card program that is targeted to the customer base of a merchant, service provider, or other commercial organization. A co-branding partner is typically a profit-based company with a recognized brand or logo. It may have merchant outlets and/or an existing card program.

Cardholder services (for example, assistance services) that are part of a Member's standard current account package are not considered to be part of Affinity or Co-branded Card Programs.

5.6 Discounts on Purchases

Except as specifically permitted in paragraph 2 below, a discount that is not available to all Cards may not be applied at a POS location solely upon presentation of an A/CB Card for payment.

The following discount practices are permitted in connection with A/CB Card programs:

a. a discount that is not provided at the time of the Transaction, but which is subsequently provided (for example, credit on current account statement, rebates, etc.);

b. a discount activated by presentation of a separate document/certificate in addition to the A/CB Card (for example, coupons, vouchers, etc.).

Promotion of discounts at the POS on purchases made with A/CB Cards is not permitted.

7.1 Acquirer Obligations and Activities

7.1.1 Signing a Merchant—POS and Electronic Commerce Only

7.1.1.2 Required Provisions

In addition to the rules in chapter 7 "Acquiring," subsection 7.1.1 in part 1 of this rulebook, the following apply:

a. clauses to be included within the merchant agreement are detailed in the *Maestro Merchant Operating Guidelines* (MOG), which are contained in appendix C of part 2 of this rulebook; and

b. Merchant pricing is at the absolute discretion of Acquirers who negotiate and contract under their own terms with Merchants to have Transactions accepted at the POS Terminals and to provide authorization, Transaction processing and fund collection services.

c. Acquirers must terminate merchant agreements promptly with Merchants who do not conform to the Rules, and the regulations, policies and technical specifications of the Organization. This conformity must include:

   1. application of the security and authorization procedures;

   2. compliance of POS Terminals to the Organization's POS Terminal specifications.

Acquirers may be instructed to terminate merchant agreements.

7.1.3 Acquiring Transactions

In addition to the requirements in chapter 7 "Acquiring," subsection 7.1.3 in part 1 of this rulebook, Acquirers must:

a. supply the Merchant with Merchant Operating Guidelines relevant to the type of Merchant and the type of POS Terminal(s) installed;

b. allocate each outlet with a merchant category code (MCC) and an outlet identity. Refer to the *Host-EM Programmer Specifications* for more details on these requirements.

7.1.5 Transmitting and Processing Transactions

In addition to the rules in chapter 7 "Acquiring," subsection 7.1.5 in part 1 of this rulebook, the following applies:

All online POI Terminals (both PIN-based and signature-based) must have on-line connection to the Acquirer host system for the authorization of all Transactions.

7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only

7.2.3 Merchant Surcharging

The following rule replaces chapter 7, "Acquiring," subsection 7.2.3 in part 1 of this rulebook:

The prohibition on Merchant surcharging in section 7.2.3 of part 1 of this rulebook does not apply in the European Economic Area.

If a Merchant applies a surcharge for payment by Card, the amount of the surcharge must be clearly indicated to the Cardholder at the POI and must bear a reasonable relationship to the Merchant's cost of accepting Cards.

7.4 Acquiring Electronic Commerce Transactions

Cross-border acquiring of electronic commerce Transactions is not currently permitted in the Region, except pursuant to the central acquiring rules in section 1.3.6 of this chapter.

7.6 Eligible POI Terminals

The following rule replaces chapter 7, "Acquiring," subsection 7.6 (b) in part 1 of this rulebook:

Acquirers may not allow access to the Organization to ATMs or PIN-based in-branch terminals owned by entities that are not eligible for membership, unless specific authorization is obtained from the Europe Region Board. Such authorization will only be granted in exceptional circumstances and on such conditions as are considered necessary. The Acquirer will have to demonstrate that it controls how the ATMs and PIN-based in-branch terminals participate in the Organization and that it accepts full liability and responsibility for the Transactions deriving from those ATMs and PIN-based in-branch terminals.

7.7 POS Terminal and Terminal Requirements

In addition to the rules in chapter 7, "Acquiring," section 7.7 in part 1 of this rulebook, the following apply:

Each Acquirer decides on the suppliers, manufacturers and model of each type of POS Terminal that it supports.

The storage of a negative file is not required.

For POS Terminals, it is recommended that screen messages, particularly at unattended POS Terminals, be available in three Cardholder selectable languages (English, French and German), plus the local language.

Terminals must offer customer prompts in English as well as in the local language. French and German must also be available whenever technically feasible. It is recommended that Spanish and Italian be offered as well. The selection of the language should be determined by the customer. Simultaneous display in two or more languages is allowed.

7.7.4 Function Keys

The following replaces the rule in chapter 7, "Acquiring," subsection 7.7.4 paragraph 1 in part 1 of this rulebook:

The function key to terminate a Transaction is mandatory.

7.7.7 Card Authentication

POS Terminals must validate the authenticity of Cards.

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

a. Longitudinal Redundancy Check (LRC)—The magnetic stripe must be read without LRC error. If the magnetic track cannot be interpreted correctly, the Transaction is neither performed nor recorded;

b. Track Layout—The track layout must conform to the specifications in appendix B of this rulebook. If this is not the case, the Card is not valid and the Cardholder must be advised. The attempted Transaction does not have to be recorded.

7.8 Hybrid POS Terminal and Hybrid Terminal Requirements

In addition to the rules in chapter 7, "Acquiring," section 7.8 in part 1 of this rulebook, the following applies:

Acquirers must be capable of carrying the full set of Issuer application data as defined in EMV (that is, up to 32 bytes) for chip Transactions.

7.9 Additional Requirements for POS Terminals

7.9.1 Additional Requirements for Hybrid POS Terminals

In addition to the rules in chapter 7, "Acquiring," subsection 7.9.1 in part 1 of this rulebook, the following apply:

No Liability Shift at Online Capable Hybrid POS Terminals

The Issuer of magnetic stripe-only Cards has no right to charge back under reason code 4870 fraudulent magnetic stripe Transactions completed with online PIN as the CVM at EMV-compliant online capable hybrid POS Terminals.

No Liability Shift at Offline-PIN-Only Hybrid POS Terminals

The Issuer of magnetic stripe-only Cards has no right to charge back under reason code 4870 fraudulent Transactions completed with signature as the CVM at offline-PIN-only hybrid POS Terminals located in a country that has a waiver permitting the support of such POS Terminals (refer to Part 1, section 7.9.1).

Technical Fallback

If both the Card and POS Terminal are hybrid, the Transaction must first be attempted using the chip.

Only if the chip cannot be used to complete the Transaction may the Transaction be initiated with the magnetic stripe. Magnetic stripe Transactions undertaken by hybrid Cards at hybrid POS Terminals must be authorized online to Issuer with PIN (signature if acquired in a Signature Waiver country (refer to Part 1, section 6.4.3).

The Issuer does not have the right to charge back under reason codes 4526 or 4870 fraudulent fallback magnetic stripe Transactions completed with online authorization. If a fraudulent fallback Transaction is completed in any other way, the Issuer has the right to charge back the Transaction, using reason code 4870.

CVM Fallback

CVM fallback (that is, from PIN to signature on a Chip Transaction) is not permitted.

7.9.1.1 Hybrid POS Terminal CAM Policy

In addition to the rules in chapter 7, "Acquiring," subsection 7.9.1.1 in part 1 of this rulebook, the following applies:

All online capable hybrid POS Terminals must support dynamic online CAM.

7.12 POI Terminal Transaction Log

In addition to the rules in chapter 7, "Acquiring," section 7.12 in part 1 of this rulebook, the following apply:

POS Terminal Transaction Log

All Transactions (successful or unsuccessful) which generate a message or Transaction code have to be sequentially registered in a transaction file. This can be done at the point-of-sale itself or at a central location either on paper or electronically. The Transaction records have to be available on request in printed form for two (2) years after the Transaction.

Acquirers must supply Transaction printouts to Issuers on request. Either original or legally acceptable copies may be supplied. Please refer to appendix D of the *European Chargeback Guide* for the retrieval request procedure. Once any claim or dispute is raised on a Transaction, all documents relating to that Transaction must be kept until such a claim or dispute is resolved.

The following data must be provided by the Acquirer in the Transaction record:

- POS Terminal identification
- Transaction date
- Transaction time
- Transaction code
- point of service condition code
- merchant category code
- response code
- Transaction amount (in local currency)
- Issuer identification
- full PAN
- Card sequence number (if applicable)
- expiration date
- Transaction number
- authorization response identifier

From among all the discretionary data, only the Card sequence number may be recorded. The PIN, however, may never be recorded.

For chip Transactions, Acquirer Transaction records should additionally contain the Transaction's cryptogram and related data elements.

Terminal Transaction Log

All Transactions (successful or unsuccessful) that generate a message or a Transaction code must be identifiable on an audit tape and contain substantially the same information as provided on the Cardholder receipt if one is provided.

On request, Acquirers must supply Transaction audit tapes or system logs to Issuers. Either original or legally acceptable copies may be supplied.

On request, Acquirers and Issuers must assist in the resolution of Cardholder disputes by providing printed copies of their records of specific Transactions.

Transaction records must be kept for two (2) years after the Transaction date or such longer period as required by local legislation. Once any claim or dispute is raised on a Transaction, all documents relating to that Transaction must be kept until the claim or dispute is resolved.

Acquirer Transaction records should contain the following data to enable matching of the audit tape to the original Transaction:

- Terminal identification
- Transaction date
- Transaction time
- Transaction code
- point of service condition code
- response code
- Transaction amount
- currency denomination
- withdrawal amount (in local currency)
- full track 2 data including PAN, card sequence number, and expiration date
- Transaction number
- authorization response identifier.

The PIN must never be recorded in the clear or in encrypted form.

For chip Transactions, Acquirer Transaction records should additionally contain the Transaction's cryptogram and related data elements.

7.13 Requirements for Transaction Receipts

In addition to the rules in chapter 7, "Acquiring," section 7.13 in part 1 of this rulebook, the following apply:

Signature-based POS Terminals must generate a receipt for each Transaction.

Terminals should provide a Transaction receipt upon Cardholder request or automatically, providing the Terminal can support this function. Cash withdrawals without receipts are allowed when the device is out of service or out of paper, the Cardholder being duly advised.

The Transaction amount may be indicated in a different currency printed at the bottom of the receipt with a clear indication that it is being provided only for information purposes. A maximum of two currencies may be indicated on a receipt.

7.13.1 Receipt Contents for POS Terminals

In addition to the rules in chapter 7 "Acquiring," subsection 7.13.1 in part 1 of this rulebook, the following apply:

The Transaction receipt should contain the following data:

Merchant Details

a. merchant identification (mandatory)

b. merchant trading address (optional)

c. merchant outlet identifier (Acquirer's) (mandatory)

d. VAT registration number (optional)

Card Scheme Details

a. space for card scheme name—'Maestro' (configurable) (mandatory)

Transaction Details

a. local date and time of the Acquirer (DD/MM/YY, HH.MM - 24 hr) (mandatory)

b. Transaction printout (receipt) number (optional)

c. POS Terminal identification (mandatory)

d. POS Terminal location (name, city, country) (mandatory)

e. Transaction type (e.g. purchase, refund) (mandatory)

f. amount (mandatory)

g. unique Transaction number (mandatory)

h. authorization response identification (mandatory)

i. currency denomination (mandatory)

j. Transaction amount in a different currency, printed at the bottom of the receipt with a clear indication that it is being provided only for information purposes (optional)

Card Details

a. PAN recommended (must be truncated if included)

b. expiration date (recommended)

c. card sequence number (optional). Other discretionary data is not allowed.

Cardholder Interface Details (optional, variable)

a. Message to Cardholder:

   1. "Your account will be debited/credited with the above amount";
   2. "Transaction confirmed";
   3. "……." Cardholder signature (mandatory for signature-based POS Terminals);
   4. "Please keep this copy."

b. Thank you message.

7.13.4 Balance Inquiry Display

The following rule replaces chapter 7, "Acquiring," subsection 7.13.4 in part 1 of this rulebook:

The balance inquiry functionality is not currently supported in the Europe Region.

9.1 POS Transaction Types

9.1.2 Acquirer Online POS Transactions

9.1.2.1 Required Transactions

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.1.2.1 a) in part 1 of this rulebook, the following apply:

The Cardholder must verify the Transaction either by PIN or by signature.

No maximum Transaction amount applies to the purchase Transaction.

Maestro operates 'online to Issuer' for all magnetic stripe Transactions. Chip Transactions may, however, be authorized offline by the chip subject to international floor limits.

If a system failure occurs, the Transaction may be authorized in dynamic stand-in mode at Issuer discretion.

All purchase Transactions, which have been authorized by the Issuer or by its agent, are guaranteed, providing the Acquirer has fulfilled all its obligations. Transactions authorized offline by the chip are guaranteed in the same way.

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.1.2.1 b) in part 1 of this rulebook, the following apply:

Whenever an Acquirer identifies an error in the presentment of a Transaction, it must generate a reversal. There is no time limit for the Acquirer to issue a reversal, and either a full or a partial reversal may be generated, as applicable.

If a full reversal is received before the clearing record for the Transaction has been forwarded to the clearing file, the Transaction will not be included in the clearing file.

If a partial reversal is received before the clearing record for the Transaction has been forwarded to the clearing file, the Transaction will be presented with the correct resulting Transaction amount.

Please refer to the *ECCF Programmer Specifications* for further information.

9.1.2.2 Optional Online POS Transactions

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.1.2.2 in part 1 of this rulebook, the following apply:

'Scrip', 'Merchant approved Transactions', 'account selection' and 'balance inquiry' are not currently supported within the Europe Region.

'Refund' and 'cancel' functions are supported in place of 'correction'.

Pre-authorization

A pre-authorization system allows a Cardholder to pay at POS Terminals where the exact amount of the purchase is not known until the purchasing process is finalized. This is mainly required at unattended POS Terminals e.g. petrol stations, where a previous checking of availability of funds is needed in order to allow the purchase.

Internationally this type of purchase can be supported either:

a. by the use of an authorization message followed by a partial reversal. At the outset of the Transaction, the authorization message is sent for a fixed amount, called the maximum pre-authorization amount. After finalizing the purchase and when the exact purchasing amount is known, a partial reversal is sent to correct the previously authorized amount; or

b. by the use of an authorization message followed by the sending of the exact purchasing amount in the clearing record. At the outset of the Transaction, the authorization message is sent for a fixed amount, called the maximum pre-authorization amount.

In both cases, the corresponding clearing record must be presented within seven (7) calendar days.

The maximum pre-authorization amount is set by the Acquirer and may vary depending on the Merchant category and the domestic situation. The actual purchase amount cannot exceed the maximum pre-authorization amount.

For the authorization process, the Card is read only once. However, to obtain a Transaction printout it may be necessary to insert the Card again, depending on the Acquirer's domestic system.

Pre-authorization on Chip Cards

Pre-authorizations on Chip Cards must be processed in accordance with the chip technical specifications. Pre-authorizations may be completed online or offline. Once a pre-authorization has been approved, the process of clearing the subsequently completed Transaction is identical to the process following a magnetic stripe pre-authorization.

Correction

Correction is not available as a separate function in Europe. In order to correct a Merchant or Cardholder error, the 'refund' function may be used. If the Transaction was not yet completed, the 'cancel' function may be used. Please refer to applicable headings below.

Cancel

A purchase or refund Transaction may be cancelled prior to its completion by use of a "CANCEL" or "STOP" key on the POS Terminal. Within the Europe Region, every POS Terminal that supports the purchase and/or refund Transaction must have the ability to cancel a Transaction.

If the Cardholder or Merchant cancels the Transaction, or a technical failure occurs involving a magnetic stripe Transaction, either before or after the authorization request has been forwarded to the Issuer:

a. the Cardholder and Merchant must be informed;

b. there must be no record of a Transaction;

c. a reversal advice message must be reported to the Issuer. (Refer to *Host-EM Programmer Specifications*).

If after sending an authorization request, the POS Terminal does not receive a response, it has to 'time-out' and send an automatic reversal. In this case:

a. the Cardholder and Merchant must be informed;

b. the attempted Transaction must be recorded;

c. a reversal advice message must be reported to the Issuer with a response code. (Refer to *Host-EM Programmer Specifications*).

Refund

The refund Transaction allows the Merchant to refund the Cardholder, by crediting the Cardholder's Account for returned goods.

This Transaction is not mandatory for Acquirers and may not be available at every outlet. However, the refund Transaction is mandatory for Issuers who must accept credits for their Cardholders in the clearing files.

The maximum Transaction amount for refunds is the authorized Transaction amount of the corresponding purchase.

As the Issuer receives money, no Issuer authorization is required for a refund. However, the Acquirer may authorize refunds at its discretion. Cardholders should be asked for proof of purchase (receipt etc.) showing that the original Transaction was undertaken using a Card as the payment method.

A Transaction printout must be generated for a refund Transaction.

The refund Transaction is an Acquirer liability.

Clearing of refunds is done in batch mode. The clearing record contains the refund data and the interchange fee information. The interchange fee is reversed from the Issuer to the Acquirer for every refund Transaction.

Refunds on Chip Cards

For chip Transactions, refunds must be processed in accordance with the chip technical specifications. Refund Transactions do not require the Card to be authenticated, the Cardholder to be verified or online authorization.

No Transaction cryptogram will be produced for a refund Transaction.

9.1.4 Acquirer Offline POS Transactions

'Account selection' is not currently supported in the Europe Region.

9.2 Terminal Transaction Types

9.2.2 Acquirer Requirements

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.2.2 in part 1 of this rulebook, the following apply:

Transfers from one Account to another and the balance inquiry functionality are not currently supported within the Europe Region.

Reversals, where required, must be sent as soon as possible, but no later than sixty (60) seconds after the authorization response has been received at the acquiring host connected to the EM.

9.2.2.1 Acquirer—Optional Transactions

The purchase of Merchandise by Cards from no account specified is permitted in the Europe Region.

9.7 Performance Requirements

In addition to the rules in chapter 9, "Processing Requirements," section 9.7 in part 1 of this rulebook, the following apply:

Please refer to the *MasterCard Business Performance Solutions* brochure for the global minimum standards applicable to Maestro.

Updates to the global minimum standards are communicated within Europe via Europe Edition Operations Bulletins.

Rules Applicable Only to the Latin America and the Caribbean Region

Set forth below are the Rule variations to the *Maestro® Global Rules* and additional rules for the Latin America and the Caribbean region. These rules are excerpted from chapter 20, "Latin America and the Caribbean Region," of the *Maestro Global Rules*. These rules apply only to the Latin America and the Caribbean region.

5.6 Discounts on Purchases

Except as specifically permitted in paragraph 2 below, a discount that is not available to all Cards may not be applied at a POS location solely upon presentation of an A/CB Card for payment.

The following discount practices are permitted in connection with A/CB Card programs:

a. a discount that is not provided at the time of the Transaction, but which is subsequently provided (for example, credit on current account statement, rebates, etc.); and

b. a discount activated by presentation of a separate document/certificate in addition to the A/CB Card (for example, coupons, vouchers, etc.).

9.1 POS Transaction Types

9.1.2 Acquirer Online POS Transactions

9.1.2.1 Required Transactions

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.1.2.1 in part 1 of this rulebook, the following applies:

c. cancel

Acquirers and Merchants must ensure that each POS Terminal supports the electronic processing of the cancel Transaction.

9.1.2.2 Optional Online POS Transactions

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.1.2.2 (7) in part 1 of this rulebook, the following apply:

Refunds are generated by Acquirers to credit a Cardholder's Account.

Refunds may be submitted to the Interchange System up to forty-five (45) calendar days after the Settlement Date of the Transaction.

No documentation is required to be submitted with a refund.

9.6 Authorizations

9.6.2 Terminal Transaction Routing

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.6.2 in part 1 of this rulebook, the following applies:

All Transactions must be routed to the Interchange System for authorization.

Rules Applicable Only to the United States Region

Set forth below are the Rule variations to the *Maestro® Global Rules* and additional rules for the United States region. These rules are excerpted from chapter 22 of the *Maestro Global Rules*. These rules apply only to the United States region.

4.4 Display of the Service Marks at POI Terminals

In addition to the rules in chapter 4, "Service Marks," section 4.4 in part 1 of this rulebook, the following applies:

The Service Marks may appear in conjunction with other regional or national network EFT Marks on devices that qualify as POS Terminals and Terminals.

7.7 POS Terminal and Terminal Requirements

7.7.2 Manual Key-Entry of PAN

The following replaces chapter 7, "Acquiring," subsection 7.7.2 in part 1 of this rulebook:

If the POS Terminal's magnetic stripe reader is disabled or the stripe on the Card is unreadable, manual entry of the Card PAN is allowed as a fallback procedure only. The Cardholder and the Card must be physically present at the Merchant location and time of the Transaction, and the Cardholder must enter a PIN to effect the Transaction. Issuers may deny these Transactions as a result of missing data.

7.7.3 PIN Entry Device

The following replaces subsection 7.7.3 a. of chapter 7, "Acquiring," in part 1 of this rulebook:

a. have an alphanumeric keyboard to enable the entry of PINs.

The following replaces subsection 7.7.3 c. of chapter 7, "Acquiring," in part 1 of this rulebook:

c. be capable of allowing entry of PINs having from four (4) to twelve (12) characters.

7.7.6 Balance Inquiry

In addition to the rules in chapter 7, "Acquiring," subsection 7.7.6 in part 1 of this rulebook, the following applies:

Each Acquirer must ensure that a balance inquiry is initiated through the use of a PIN and a magnetic stripe reader and is performed only at Cardholder-operated POS Terminals and Terminals.

7.9 Additional Requirements for POS Terminals

In addition to the rules in chapter 7, "Acquiring," section 7.9 in part 1 of this rulebook, the following applies:

c. POS Terminals must contain keyboards that assign letter-number combinations as described in section 7.10 in part 1 of this rulebook.

7.12 POI Terminal Transaction Log

The rules in chapter 7, "Acquiring," section 7.12 in part 1 of this rulebook apply, except that the inclusion of the Transaction code description on the Transaction log is optional.

9.1 POS Transaction Types

9.1.2 Acquirer Online POS Transactions

9.1.2.1 Required Transactions

The following replaces chapter 9, "Processing Requirements," subsection 9.1.2.1 b. in part 1 of this rulebook:

Acquirers must support reversals for the full or partial amount of any authorized Transaction whenever the system is unable, because of technical problems, to communicate the authorization response to the POS Terminal.

9.1.2.2 Optional Online POS Transactions

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.1.2.2 b.2 in part 1 of this rulebook, the following applies:

Cashback must be distinguished from the purchase Transaction.

The following replaces chapter 9, "Processing Requirements," paragraph 4 of subsection 9.1.2.2 b.4. in part 1 of this rulebook:

Acquirers are not liable for pre-authorization completions that occurred within twenty (20) minutes of the initial Transaction that were stored and forwarded because of technical problems between the Acquirer and the Interchange System, or the Interchange System and the Issuer.

9.6 Authorizations

9.6.2 Terminal Transaction Routing

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.6.2 in part 1 of this rulebook, the following apply:

Whenever a Card issued in the United States is used at a Terminal in the United States and the Service Mark is a common brand, but not the only common brand, on the Card and the Terminal, the resulting Transaction must be routed to the interchange system specified by the Issuer.

The Transaction must be routed to the Interchange System unless the Issuer informs the Organization that it has specified an interchange system other than the Interchange System.

9.6.4 Authorization Response Time

9.6.4.1 Issuer Response Time Requirements

In addition to the rules in chapter 9, "Processing Requirements," subsection 9.6.4.1 in part 1 of this rulebook, the following apply:

Principal Members must respond to ninety-five (95) percent of all Transaction requests within five (5) seconds.

Additional information regarding response time standards can be found in the *MDS Online Specifications* manual.

9.6.4.2 Acquirer Response Time Requirements

The following replace chapter 9, "Processing Requirements," paragraphs 1 and 2 of subsection 9.6.4.2 in part 1 of this rulebook:

Each Acquirer is required to wait at least twenty (20) seconds before timing out a Transaction.

Each Acquirer must ensure that its POS Terminals and Terminals wait a minimum of twenty-five (25) seconds before timing out a Transaction.

13.8 Pre-authorized Transactions

The following replaces chapter 13, "Liabilities and Indemnification," paragraph 1 of section 13.8 in part 1 of this rulebook:

An Issuer is liable for any Transaction, for which the Acquirer obtained a pre-authorization, and, which the Acquirer stored and forwarded to the Issuer within twenty (20) minutes of the pre-authorization.

7 *Excerpts from* Cirrus Worldwide Operating Rules *(published June 2005)*

This chapter contains excerpts of the Cirrus Worldwide Operating Rules *manual published June 2005. This* Merchant Rules Manual *contains only information applicable to merchants; therefore, some sections provided in the* Maestro Global Rules *manual may have been omitted herein.*

Rules Applicable Only to the Europe Region

Set forth below are the Rule variations to the *Cirrus Worldwide Operating Rules* and additional rules for the Europe region. These rules are excerpted from chapter 19 of the *Cirrus Worldwide Operating Rules*. These rules apply only to the Europe region.

14.5 Card Issuing Programs

14.5.4 Payment of Fees

In addition to the rules in chapter 14, "Member Service Providers," subsection 14.5.4 in part 1 of this rulebook, the following applies:

All Cardholder fees must be paid to the Member unless the Europe Region Board permits the fees to be paid to the Member Service Provider (MSP). MasterCard Europe may authorize the MSP to collect payments from applicants and Cardholders on an interim basis, pending approval by the Europe Region Board at its next meeting.