Maestro Global Rules

9 November 2012

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary to MasterCard International Incorporated, one or more of its affiliated entities (collectively "MasterCard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

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

Disclaimer

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

Translation

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard customers. MasterCard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

Information Available Online

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on MasterCard Connect™. Go to Publications Support for centralized information.

Summary of Changes

This document reflects changes associated with announcements published in MasterCard Bulletins dated from April 2012 to November 2012. To locate these changes online, on the Adobe toolbar, click Find. In the Find box, type >>, and then press ENTER. To move to the next change, press ENTER again.

Description of Change	Where to Look
Revised Standards for fraud reporting to the System to Avoid Fraud Effectively (SAFE)	Definitions and Chapter 6
Revised Standards related to the use of Confidential Transaction Data	Chapter 3
Revised Standards to eliminate restrictions on prefixes for Primary Account Numbers (PAN)	Chapter 6
Introduced Standards that will enhance the ability of an issuer to detect fraudulent magnetic stripe transactions	Chapter 6
Revised Standards about the new acknowledgement bulk file for IPM Member Parameter Extract (MPE) and Financial Institution Table (FIT)	Chapters 7 and 9
Revised Standards for Support of the Device Type Indicator	Chapters 6 and 20
Revised Standards for acquirers in the Europe region to reflect that they are no longer required to support technical fallback at attended point-of-sale (POS) terminals; however, MasterCard recommends that fallback support is withdrawn only after the acquirer's chip infrastructure is robust and customer service will not be adversely affected.	Chapters 7, 9, 17
Introduced Standards to support the processing of Russian domestic MasterCard® *MoneySend*™ payment transactions funded with cash or other anonymous funding sources	Chapters 7, 9, and 17
Modified Standards to relax requirements relating to screening performed by acquirers when beginning to do business with an acquirer	Chapter 7
Revised Standards related to Account Data Compromise (ADC) Events and potential ADC Events	Chapter 8
Revised Standards for *PayPass* and QPS Transactions in Cyprus	Chapter 9
Introduced Standards about settlement finality in the Europe region	Chapters 10 and 17
Revised Standards on participation for some countries in the Asia/Pacific region	Chapter 15
Revised Standards pertaining to the Maestro® Marks on cards	Chapters 15, 18, and 20
Modified Standards to include authorization message mandates for Italy	Chapter 17
Introduced Standards about limited cardholder liability. The rules are mandatory in the European Economic Area (EEA) and are recommended to be followed by customers in other Europe region countries.	Chapter 17

Description of Change	Where to Look
Modified interchange Standards to specify that point-of-sale (POS) transactions must be submitted with the interchange rate designator for the lowest fee tier that applies for those transactions	Chapter 17
Modified Standards to allow *PayPass* transactions to be permitted above the current *PayPass* transaction ceiling limit throughout the Europe region provided online PIN verification occurs	Chapter 17
Clarified Europe region Standards related to using recurring payments for bill payments	Chapter 17
Revised Standards for Gaming Payment Transaction in Europe	Chapter 17
Modified Standards to support the MasterCard *MoneySend* program in Belarus	Chapter 17
Revised Standards to extend ATM balance inquiry and/or PIN management services mandate to additional countries: Albania, Armenia, Belarus, Bosnia, Kosovo, Macedonia, Moldova, Montenegro, and Serbia Please note that this rule is effective 15 November 2012.	Chapter 17
Clarified the application of the central acquiring rules to the Payment Facilitator Mode in Europe	Chapter 17
Revised Standards for interregional Payment Transactions acquired in the Europe region and conducted with a Maestro card issued in another region	Chapter 17
Modified rules related to MO/TO domestic transactions in Turkey	Chapter 17
Revised Standards for Maestro *PayPass* and Maestro contactless magnetic stripe transactions	Chapter 18
Revised Standards to reflect mandates related to Payment Transactions, applicable in the South Asia/Middle East/Africa region	Chapter 19
Revised Standards to support the MasterCard U.S. Region Point-of-Interaction (POI) Roadmap	Chapter 20
Revised Standards related to debit PIN POS functionality in the United States	Chapter 20
Revised Standards for the registration of U.S. region merchants that conduct skill games	Chapter 20
Clarified the requirements for *PayPass* readers deployed at U.S. region merchants, and chargeback applicability for issuers relating to PIN support on EMV chip cards	Chapter 20
Revised Standards to permit Maestro® *PayPass*™-only acceptance at mass events, festivals and sports arenas in Hungary and the United Kingdom, subject to approval on a case-by-case basis	Chapter 21
Revised Standards to include three new card acceptor business codes (MCCs) for Maestro *PayPass*-only acceptance at mass events, festivals, and sports arenas	Chapter 21
Other clarifications and editorial corrections as necessary	Throughout document

Table of Contents

Definitions

The following terms used in the *Maestro Global Rules* have the meaning set forth below. Commonly used industry terms are in the Glossary.

NOTE

Additional defined terms appear in Chapter 15, "Asia/Pacific Region," Chapter 17, "Europe Region," Chapter 18, "Latin America and the Caribbean Region," Chapter 19, "South Asia/Middle East/Africa Region," and Chapter 20, "United States Region," of this rulebook.

Access Device

A means other than a Card by which a Cardholder may access eligible Accounts at a POS Terminal in accordance with the Standards. *See* Card.

Account

Any checking, savings, NOW, current, sight deposit, share draft accounts (and overdraft lines of credit linked to such accounts), or pooled accounts (linked to a Corporation-approved prepaid Card Program), which are maintained by or on behalf of a Cardholder with an Issuer, and which may be accessed by a Card issued by such Issuer, for processing Transactions initiated by such Cardholder.

NOTE

A regional definition of this term appears in Chapter 17, "Europe Region," of this rulebook.

Account in Good Standing

A request that is a non-financial Transaction sent by an electronic commerce or Mobile Remote Payment Merchant to verify that the Maestro Primary Account Number (PAN) is authentic and related to a valid Account. This Transaction type does not verify the availability of funds.

Acquirer

A Customer in its capacity as an acquirer of a Transaction conducted at a POI Terminal.

Acquirer Domain Mobile Remote Payment Transaction

An Acquirer Domain Mobile Remote Payment Transaction is conducted pursuant to a program in which the Acquirer provides the offering and controls the registration of Cardholders who wish to participate. The Acquirer or its Service Manager verifies registered Cardholder accounts and the Cardholder is authenticated at the time of the transaction by credentials that have been delivered at the time of the registration, verifiable to the Service Manager.

Acquiring-only Member, Acquiring-only Customer

A type of Affiliate Member or Principal Member as referenced in Chapter 1 of this rulebook. "Acquiring-only Customer" and "Acquiring-only are alternative terms for Acquiring-only Member.

Activity(ies)

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

Affiliate Member, Affiliate Customer

An entity that is eligible and approved to be a Member pursuant to Chapter 1 of this rulebook and is Sponsored by a Principal Member. "Affiliate Customer" and "Affiliate" are alternative terms for Affiliate Member.

Approved Merchandise Category

Any category of Merchandise approved by the Corporation for sale at ATMs. A list of Approved Merchandise Categories is published in Chapter 7 of this rulebook.

Area of Use

The country or countries in which a Customer is Licensed to use the Mark(s), and, as a rule, set forth in the License or in an exhibit to the License.

ATM Access Fee

A fee charged by an Acquirer in connection with a cash withdrawal, or Shared Deposit Transaction initiated at the Acquirer's ATM with a Card, which fee is added to the amount of the Transaction transmitted to the Issuer.

Automated Teller Machine (ATM)

An unattended self-service Terminal that performs basic banking functions such as accepting deposits, cash withdrawals, ordering transfers among accounts, loan payments and account balance inquiries.

Board, Board of Directors

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

Brand Fee

A fee charged for certain Transactions not routed to the Interchange System.

Card

A card issued by a Customer enhanced with a Mark, pursuant to License and in accordance with the Standards, that provides access to an Account. Unless otherwise stated herein, the Standards applicable to a Card are applicable to an Access Device and a Mobile Payment Device.

Card Validation Code (CVC)

CVC 1 is a three-digit value encoded on tracks 1 and 2 in three contiguous positions in the discretionary data field of a magnetic stripe on a Card. Chip CVC is a three-digit value encoded in the track 2 equivalent field in three contiguous positions in the discretionary data field of a chip on a chip-enabled Card. The CVC is intended to inhibit the alteration or misuse of Card data and enhance the authentication of the Card.

Cardbase

All Cards issued bearing the same major industry identifier, BIN/IIN, and any following digits that uniquely identify Cards for routing purposes.

Cardholder

The authorized user of a Card issued by a Principal or Affiliate.

Cardholder Communication

Any communication by or on behalf of an Issuer to a Cardholder or prospective Cardholder. A solicitation is one kind of Cardholder Communication.

Chip Card (Smart Card, Integrated Circuit Card, IC Card, or ICC)

A Card with an embedded EMV-compliant chip containing memory and interactive capabilities used to identify and store additional data about a Cardholder, Cardholder's Account, or both.

Chip CVC

See Card Validation Code.

Competing EFT POS Network

A Competing EFT POS Network is a network, other than any network owned and operated by the Corporation, which provides access to Accounts at POS Terminals by use of payment cards, which possess the following characteristics:

1. provides a common service mark(s) to identify the POS Terminal and payment cards, which provide Account access;
2. it is not an affiliate of the Corporation; and
3. operated in at least one (1) country in which the Corporation has granted a License(s).

The following networks are designated without limitation to be Competing EFT POS Networks:

1. Interlink;
2. Electron; and
3. Delta;
4. V-Pay

Control

As used herein, Control has such meaning as the Corporation deems appropriate in its sole discretion given the context of the usage of the term and all facts and circumstances the Corporation deems appropriate to consider. As a general guideline, Control often means to have, alone or together with another entity or entities, direct, indirect, legal, or beneficial possession (by contract or otherwise) of the power to direct the management and policies of another entity.

Corporation

MasterCard International Incorporated, Maestro International Inc., and their subsidiaries and affiliates. As used herein, Corporation also means the President and Chief Executive Officer of MasterCard International Incorporated, or his or her designee, or such officer(s) or other employee(s) responsible for the administration and/or management of a program, service, product, system or other function. Unless otherwise set forth in the Standards, and subject to any restriction imposed by law or regulation or by the Board or by the MasterCard Incorporated Certificate of Incorporation or by the MasterCard International Incorporated Certificate of Incorporation (as each such Certificate of Incorporation may be amended from time to time), each such person is authorized to act on behalf of the Corporation and to so act in his or her sole discretion.

Cross-border Transaction

A Transaction that originates via a Point-of-Interaction (POI) Terminal located in a different country from the country in which the Card was issued.

Customer

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

Customer Report

Any report a Customer is required to provide the Corporation, whether on a one-time or repeated basis, pertaining to its License, Activities, use of any Mark, or any such matters. By way of example and not limitation, the Quarterly MasterCard Report (QMR) is a Customer Report.

CVC 1

See Card Validation Code.

Data Storage Entity (DSE)

A Service Provider that performs any one or more of the services described in Rule 14.1 of this rulebook as DSE Program Service.

Dual Interface Hybrid POS Terminal

A Hybrid POS Terminal that is capable of processing both Maestro *PayPass* Transactions by means of its contactless interface, in addition to processing contact chip Transactions by means of its contact interface. Dual Interface Hybrid POS Terminals include, but are not limited to, those which support mobile contactless chip Transactions by means of near field communications (NFC) technology.

Electronic Money

Electronically (including magnetically) accessed monetary value as represented by a claim on the Electronic Money Issuer which:

1. Is issued on receipt of funds for the purpose of making transactions with payment cards; and
2. Is accepted by the Electronic Money Issuer or a person other than the Electronic Money Issuer.

Electronic Money Issuer

An Electronic Money Institution with respect only to its issuing activities.

Electronic Money Institution

An entity authorized by applicable regulatory authority or other government entity as an "electronic money institution", "e-money institution", "small electronic money institution", or any other applicable qualification under which an entity is authorized to issue or acquire Electronic Money transactions under applicable law or regulation.

Gateway

The card used to effect the ATM Transaction is not a Card and the ATM Transaction is processed by the Interchange System.

Gateway Customer

Any Customer that uses the services of the Gateway Switch.

Gateway Processing

A service available to Customers, which:

1. Allows Processors to forward acquired ATM Transactions to the Interchange System, that will in turn be routed to issuers, that are not Customers; or
2. Allows that Interchange System to forward non-MasterCard/Maestro ATM Transactions to Processors

Gateway Switch

The computer-based system provided by the Corporation to forward non-MasterCard/Maestro acquired ATM Transactions to Processors.

Gateway Transaction

Any ATM transaction processed through or using the Gateway Switch.

Hybrid Terminal

A Terminal that:

1. is capable of processing both chip Transactions and magnetic stripe Transactions;
2. has the equivalent hardware, software, and configuration as a Terminal with full EMV Level 1 and Level 2 type approval status with regard to the chip technical specifications; and
3. has satisfactorily completed the Corporation's Terminal Integration Process (TIP) in the appropriate environment of use.

Hybrid POS Terminal

A POS Terminal that:

1. is capable of processing both chip Transactions and magnetic stripe Transactions;
2. has the equivalent hardware, software, and configuration as a POS Terminal with full EMV Level 1 and Level 2 type approval status with regard to the chip technical specifications; and
3. has satisfactorily completed the Corporation's Terminal Integration Process (TIP) in the appropriate environment of use.

Identity Standards

The visual graphics requirements adopted by the Corporation and revised from time to time, which define the correct use of the Marks on all surfaces and mediums.

Independent Sales Organization (ISO)

A Service Provider that performs any one or more of the services described in Rule 14.1 of this rulebook as ISO Program Service.

Interchange System

The computer hardware and software operated by and on behalf of the Corporation for the routing, processing, and settlement of Transactions including, without limitation, the MasterCard Worldwide Network, the Regional Service Centre [RSC], the Global Clearing Management System (GCMS), and the Settlement Account Management (SAM).

Interchange System Business Day

The period of processing time from cutover to cutover.

Intermediate network facility (INF)

Any message-processing entity positioned between the Acquirer of a Transaction and the Issuer, including a Service Provider and the Interchange System.

Interregional Transaction

A Transaction that originates via a POI Terminal located in a different Region from the Region in which the Card was issued.

Intracountry Transaction

A Transaction that originates via a POI Terminal located in the same country as the country in which the Card was issued.

Intraregional Transaction

A Transaction that occurs at a POI Terminal located in a different country from the country in which the Card was issued, within the same Region.

Issuer

A Customer in its capacity as an issuer of a Card.

Issuer Domain Mobile Remote Payment Transaction

An Issuer Domain Mobile Remote Payment Transaction is conducted pursuant to a program in which the Issuer provides the offering and controls the registration of Cardholders who wish to participate. The Issuer or its Service Manager verifies registered Cardholders and the Cardholder is authenticated at the time of the transaction by credentials that have been delivered at the time of the registration, verifiable by the Service Manager or the Issuer.

License, Licensed

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

Licensee

A Customer or other person authorized in writing by the Corporation to use the Maestro Mark(s).

Maestro

Maestro International Incorporated, a Delaware USA corporation or any successor thereto.

Maestro® *PayPass*™

Maestro *PayPass* is a contactless payment functionality that uses radio frequency ("RF") technology to exchange Transaction data between a Chip Card, an Access Device, or a Mobile Payment Device, and a RF-enabled POS Terminal that bears the Maestro *PayPass* logo. Maestro *PayPass* provides Cardholders with an option to purchase goods or services at or below the applicable Transaction amount ceiling limit without entering a PIN or signing the Transaction receipt.

Maestro Word Mark

The Maestro Word Mark is represented by the word "Maestro" followed by a registered trademark ® or ™ symbol (depending on its trademark status in a particular country) or the local law equivalent. Maestro is the exclusive owner of the Maestro Word Mark.

Marks

The Maestro names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks that Maestro International Inc, MasterCard International Incorporated and/or their affiliates or subsidiaries own, manage, license, or otherwise Control and make available for use by Customers and other authorized entities in accordance with a License. A "Mark" means any one of the Marks.

MasterCard

MasterCard International Incorporated, a Delaware U.S.A. corporation.

MasterCard Europe

MasterCard Europe sprl, a Belgian private limited liability (company).

MasterCard Incorporated

MasterCard Incorporated, a Delaware U.S.A. corporation.

Member

A financial institution or other entity that has been granted a License in accordance with the Standards. A Member is also referred to as a Customer.

Merchandise

Any merchandise, service, or other thing of value for purchase, other than currency, dispensed or otherwise provided at an ATM, within an Approved Merchandise Category and conforming to the requirements of Chapter 7 of this rulebook.

Merchandise Transaction

A Transaction conducted at an ATM associated with the purchase of Merchandise by a Cardholder.

Merchant

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

Merchant Agreement

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

Merchant ID Number

A unique number assigned by the Acquirer to identify the Merchant.

Mobile Device for Personal PIN Entry

A Cardholder-controlled mobile phone that has been registered either with the Cardholder's Issuer and is used for entry of the Cardholder's credentials, such as the Card PIN or Issuer assigned mobile-specific credentials, or with the Acquirer or its agent and is used for entry of the Cardholder's Acquirer Domain Mobile Remote Payment Transaction-assigned mobile-specific credentials. Within the Acquirer Domain, the Card PIN is not allowed to be used. Refer to the *Mobile Remote Payments Program Guide* for more information.

Mobile Payment Device

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

Mobile Remote Payment Transaction

A Mobile Remote Payment Transaction is a financial Transaction that is initiated and authenticated by an enrolled Cardholder from the Cardholder's Mobile Device for Personal PIN Entry.

Multiple or Partial Delivery

A process by which an electronic commerce Merchant completes a single purchase order made by a Cardholder, by making more than one delivery and more than one partial payment charge.

NICS™

The system utilized by the Corporation to gain access to and interface with certain database information at the Interchange System.

Ownership

As used herein, ownership has such meaning as the Corporation deems appropriate in its sole discretion given the context of the usage of the term in all facts and circumstances the Corporation deems appropriate to consider. As a general guideline, ownership often means to own indirectly, legally, or beneficially more than fifty percent (50%) of an entity.

Payment Facilitator

A Merchant registered by an Acquirer to facilitate Transactions on behalf of Sub-merchants. Unless otherwise stated herein, any reference to Merchant(s) encompasses Payment Facilitator(s) and Sub-merchant(s). The Standards applicable to a Merchant are applicable to a Payment Facilitator and a Sub-merchant.

Payment Transaction

A Payment Transaction is a Transaction that transfers funds from a Merchant (MCC 6533) or Customer (MCC 6532) to an Account.

PIN-based In-Branch Terminal

An attended POI device, located on the premises of a Customer financial institution or on the premises of a financial institution designated as an authorized agent by the Corporation that facilitates a cash withdrawal Transaction by a Cardholder.

POI Terminal

Any attended or unattended POI device that meets the Corporation requirements and that permits a Cardholder to initiate and effect a Transaction in accordance with the Rules.

Point of Interaction

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

POS Terminal

An attended or unattended POI device located in or at a Merchant's premises that meets the Corporation's requirements, and that permits a Cardholder to initiate and effect a Transaction for the purchase of goods or services sold by such Merchant with a Card in accordance with the Rules.

Primary Operations Contact

The individual designated in writing to the Corporation by the Principal as a person authorized to represent the Principal.

Principal Member, Principal

An entity that is eligible and approved to be a Member pursuant to Chapter 1 of this rulebook. "Principal" is an alternative term for Principal Member. A Principal Member is also referred to as Customer.

Processed Transaction

A Transaction for which:

- the Issuer or its agent approved the Acquirer's request to proceed ("authorization") by means of the Interchange System, unless both the Terminal and the chip approved the offline authorization of a chip Transaction;
- the exchange of Transaction record data between Customers ("clearing") occurred by means of the Interchange System; and
- the exchange of funds between Customers ("settlement") occurred by means of the Interchange System.

Program

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

Program Service(s)

Any service described in Rule 14.1 of this rulebook that directly or indirectly supports a Program. The Corporation has the sole right in its sole discretion to determine whether a service is a Program Service.

Region

A distinct geographic territory encompassing the location of multiple Customers as defined by the Corporation from time to time.

Regional Service Centre (APC/RSC)

One of the computer-based systems provided by the Corporation in accordance with the Rules, servicing Australia.

Rules

The Standards set forth in the *Maestro Global Rules* manual.

Service Manager

A Service Provider that has been approved by the Corporation to provide Mobile Remote Payment Transaction Program Service.

Service Provider

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

Service Provider Registration Facilitator

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

Settlement

The process by which Customers exchange financial data and value resulting from Transactions.

Settlement Date

Date that funds are committed for settlement between an Acquirer and an Issuer.

Settlement Obligation

A financial obligation of a Principal Customer to another Principal Customer arising from a Transaction.

Shared Deposit

A deposit Transaction to a savings Account or checking Account conducted at a Terminal located in the U.S. region initiated with a Card issued by a U.S. region Customer other than the Acquirer.

Smart Card

See Chip Card.

Solicitation, Solicit

An application, advertisement, promotion, marketing communication, or the like intended to solicit the enrollment of a person as a Cardholder or as a Merchant. To "Solicit" means to use a Solicitation.

Special Issuer Programs

Issuer Activity the Corporation deems may be undertaken only with the express prior consent of the Corporation. As of the date of the publication of these Rules, Special Issuer Programs include Affinity Card Co-Brand Card, and prepaid Card Programs.

Sponsor, Sponsorship

The relationship described in the Standards between a Principal and an Affiliate that engages in Activity indirectly through the Principal. In such event, the Principal is the Sponsor of the Affiliate and the Affiliate is Sponsored by the Principal. "Sponsorship" means the Sponsoring of a Customer.

Standards

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

Stand-In Parameters

A set of authorization requirements established by the Corporation or the Issuer that are accessed by the Interchange System using the Stand-In Processing Service to determine the appropriate responses to authorization requests.

Stand-In Processing Service

A service offered by the Corporation in which the Interchange System authorizes or declines Transactions on behalf of and uses Stand-In Parameters provided by the Issuer (or in some cases, by the Corporation). The Stand-In Processing Service responds only when the Issuer is unavailable, the Transaction cannot be delivered to the Issuer, or the Issuer exceeds the response time parameters set by the Corporation.

Sub-merchant

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

Terminal

An attended or unattended access device that meets the Corporation requirements and that permits a Cardholder to initiate and effect a Transaction at an ATM or PIN-based In-Branch Terminal with a Card in accordance with the Rules.

Third Party Processor (TPP)

A Service Provider that performs any one or more of the services described in Rule 14.1 of this rulebook as TPP Program Service.

Transaction

A series of related messages processed through the Interchange System or another Intermediate Network Facility in accordance with the Standards and not defined as a proprietary transaction.

Chapter 1 Participation

This chapter contains information about Participation in Corporate Activities.

1.1 Types of Customers

The Corporation has the following two types of Customers: Principal and Affiliate.

1.1.1 Principal

A Principal is a Customer that participates or proposes to participate directly in the Activities of the Corporation. Subject to Rule 1.6.5 Principals, regardless of whether they are an Acquiring-only Principal, may Sponsor both Affiliates that issue or propose to issue Cards and Acquiring-only Affiliates.

1.1.2 Affiliate

An Affiliate is a Customer that participates or proposes to participate indirectly (i.e., through a Principal Sponsor) in the Activities of the Corporation.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," and a regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

1.2 Eligibility to be a Customer

Entities participating in the Corporation are Customers. Entities that are eligible to become Customers are described in this subsection. In addition to all other eligibility requirements, each Customer must have the requisite right, power and authority, corporate and otherwise, to become a Customer and participate in the Corporation Activities.

1. **United States Region**. In the United States Region, as defined in the Rules, the following entities area eligible to be Customers:

    a. United States Financial Institutions. Any of the following depository institutions: a national banking or state banking association, commercial bank, savings bank, mutual savings bank, savings and loan association, credit union, or similar depository institution, as well as any entity that qualifies under § 1841(c)(2)(F) of the Bank Holding Company Act, as amended from time to time ("a § 1841 entity"), which depository institution or § 1841 entity conducts business in any of the fifty States of the United States of America or the District of Columbia and is organized under the laws of the United States of America, any State thereof, or the District of Columbia, (a) the deposits of which are eligible to be, and are, insured or guaranteed by an agency or instrumentality of the federal government of the United States of America or by similar agencies or instrumentalities of the government of any State thereof where such institution is chartered; or (b) the deposits of which are privately insured and are eligible to be insured or guaranteed by an agency or instrumentality of the federal government of the United States of

America or by similar agencies or instrumentalities of the government of any State thereof where such financial institution is chartered, and which financial institution has funded an account against its unwillingness or inability to meet its obligations to Maestro USA, in an amount and form determined, from time to time, by Maestro USA to be adequate. Financial institutions qualifying to be a Customer under clause (b) of this Rule 1.2.1 (1.a) will be permitted to participate only as Affiliates.

b. Holding Companies. Any holding company registered under the Bank Holding Company Act or the Savings and Loan Holding Company Amendments of 1967, each as amended from time to time (a "Holding Company"), two-thirds or more of the assets of which consists of the voting stock of one or more United States Financial Institution(s); and

c. EFT Interchange Networks. Any corporation, Corporation, association, or other entity which does not itself issue debit cards and which is directly or indirectly Controlled by one or more United States Financial Institutions or Holding Companies and which is engaged in operating a regional network, a primary function of which is to facilitate on-line automatic teller machine and/or point-of-sale debit electronic funds transfers among its participants, and which interchanges debit transactions in a region of the United States and uses a common regional service mark in connection therewith ("an EFT Interchange Network").

d. National Credit Union Association. Any national Corporation or association, that does not itself issue debit cards, that is directly or indirectly owned and Controlled by credit unions, and that engages in the processing of electronic funds transfers, a primary function of which is to promote the Program to its members and to facilitate education and communication regarding the marketing activities, operations, Participation Rules, and Operating Rules of Maestro.

e. Other Entities. Any entity that MasterCard (or a wholly owned subsidiary thereof) determines to be eligible to become a Customer.

2. **Canada Region**. In the Canada Region, as defined in the Rules, the following entities are eligible to be Customers:

a. Any financial depository institution conducting business in Canada that is eligible pursuant to Canadian law to participate in the Canadian clearing and settlement system.

b. Any corporation, Corporation, association, or other entity which does not itself issue debit, credit, or charge cards and which is directly or indirectly Controlled by one or more Canadian financial institutions and which is engaged, or proposes to engage, in operating a data processing network, a primary function of which is to facilitate electronic funds transfers among its members.

c. Any corporation, Corporation, association or other entity which:

i. is not Controlled by one or more financial institutions;

ii. operates the equivalent of an EFT interchange system within a geographical subset of Canada, under a retail brand name;

iii. processes transactions for such system;

iv. does not issue debit, credit or charge cards;

v. does not own credit or charge card accounts receivable; and

vi. does not own or control ATMs

provided that such entities obtain from a financial depository institution acceptable to the Corporation a stand-by letter of credit issued in favor of the Corporation in an amount determined by the Corporation from time to time to be sufficient to ensure the discharge of all such entities' obligations to the Corporation

d. Any corporation, Corporation, association or other entity, which does not itself issue debit cards, or own credit or charge card accounts receivable, and which is directly or indirectly Controlled by one or more Canadian financial institutions, and which is engaged in or proposes to engage, as a substantial portion of its business, in a credit card processing or servicing operation.

In addition to the requirements above, to be a Principal in Canada, an entity must be:

i. a Principal of MasterCard in the Canada Region; or

ii. an entity that is eligible to maintain a settlement account with the Bank of Canada (or is a participant of a group that is eligible to maintain such an account); or

iii. in the case of an EFT Interchange System owned by Financial Institutions (as described in paragraph c.ii above) or a credit card Processor (as described in paragraph c.iv above), an entity that is Controlled by a least one (1) Financial Institution that is eligible to maintain a settlement account with the Bank of Canada (or is a participant of a group that is eligible to maintain such an account)

3. **Europe Region**. In the Europe Region, as defined in the Rules, the following are eligible to become Customers:

a. any entity that is a financial institution that is authorized to engage in financial transactions under the laws and/or government regulations of the country, or any subdivision thereof, in which it is (i) organized or (ii) principally engaged in business. "Financial transactions" for purposes of this section shall mean the making of commercial or consumer loans, the extension of credit, the effecting of transactions with payment services cards, the issuance of travelers cheques, or the taking of consumer or commercial deposits.

Any such financial institution also must be regulated and supervised by one or more governmental authorities and/or agencies authorized and empowered to establish and/or enforce rules regarding financial transactions and the financial condition, activities, and practices of entities engaging in such financial transactions.

With respect to any financial institution that does not take deposits, it shall be a further requirement that financial transactions constitute substantially all of the business conducted by such institution. In the EEA it is not required that financial transactions constitute substantially all of the business conducted by a financial institution that does not take deposits.

b. Any entity that is directly or indirectly Controlled by one or more Customers described in the preceding section and that is engaged, or proposes to engage, on behalf of or through one or more of those Customers in operating programs utilizing one or more of the Marks or in related Activities.

4. **South Asia/Middle East/Africa, and Latin America and the Caribbean Regions**. In the Regions of South Asia/Middle East/Africa, and Latin America and the Caribbean, as defined in the Rules, the following entities are eligible to be Customers:

   a. Any financial depository institution that is conducting business in a country within the South Asia/Middle East/Africa Region, or the Latin America and the Caribbean Region, and that is properly constituted and regulated according to the national legislation of the country where it is located.

   b. Any corporation, Corporation, association or other entity which operates or proposes to operate a payment system, and which is located in the South Asia/Middle East/Africa Region, or the Latin America and the Caribbean Region, and is Controlled by one (1) or more regional financial institutions within such Region.

5. **Asia/Pacific**. In the Asia/Pacific Region, as defined in the Rules, the following are eligible to become Customers:

   a. Any financial institution located within the Asia/Pacific Region or entities described in paragraph (5.b) below. A financial institution is a Corporation that is authorized by the relevant regulatory authority within its country of operation to accept consumer deposits which are held in current accounts and which the financial institution may access directly on authorization from its customer. Financial institutions must meet established financial criteria that demonstrate their ability to meet their financial obligations to the Corporation.

   b. Any entity within the Asia/Pacific Region that is not a financial institution as defined in paragraph (5.a) above, but which, based on (i) the structure of the payments services market in the country, and (ii) the entity's status and/or proposed role therein, satisfies the Corporation that it is in the Corporation's best interests to authorize it to acquire Transactions, is eligible to be an Acquiring Customer as defined in the Rules. Such an entity must meet established financial criteria that demonstrate its ability to meet its financial obligations to the Corporation

6. **Licensees of MasterCard**. Upon application to and approval by the Corporation, any Licensee of MasterCard is eligible to be a Customer.

7. **Foreign Branches**. Any branch of a financial institution that is a Customer, which is located in a country other than the country where such Customer has its principal place of business, will for all purposes related to participation in the Corporation, be deemed a separate financial institution located in the foreign country. Benefits and obligations arising from the financial institution's participation in the Corporation will not accrue to or bind the foreign branch. Eligibility of the foreign branch for participation in the Corporation will be determined by reference to the Rules regarding financial institutions that are primarily engaged in business in the country where the foreign branch is located.
8. **MasterCard**. MasterCard and its successors, or any wholly owned subsidiary designated by MasterCard, is eligible to be a Customer.
9. **Exception**. Notwithstanding the eligibility criteria in subsections 1 through 7 of this Rule 1.2 an entity which is engaged in providing financial services in a country is eligible for participation in such country if the Corporation, in its sole discretion, deems that its participation is necessary to compete successfully and that such participation will promote the purposes of the Corporation.

1.3 Application to be a Customer

Any entity eligible to be a Customer may apply to become a Customer. An application to become a Customer must be made in the form and include all of the information then required, and the entity must pay the fee or fees then required. An applicant to be a Customer must agree, and by execution and submission of an application to be a Customer agrees, that it will comply with all applicable provisions of the Standards of this Corporation as in effect from time to time, and with applicable law.

1.3.1 Changing Customer Status

In the event that:

1. An Affiliate wishes to become a Principal; or
2. A Principal wishes to become an Affiliate

it must notify the Corporation and submit such information as the Corporation deems necessary. It is within the Corporation's sole discretion whether to grant the requested change in Customer status. In the event that the Corporation grants the requested change, it will assess the appropriate fee.

NOTE

Regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," of this rulebook.

1.4 Interim Participation

Pending action on a properly completed and submitted application to be a Customer, the Corporation may authorize the applicant to participate in Activity on an interim basis as if the applicant were a Customer. The continuation of such interim participation is subject to the subsequent approval or disapproval of the application to be a Customer. As a condition of such conditional authorization, the applicant must agree, and by commencement of any Activity the applicant is deemed to have agreed, to comply during this interim period (and thereafter as applicable) with the Standards and to discontinue immediately any use of the Marks and Activity if the application is disapproved. All damages, losses, costs, and liabilities arising directly or indirectly, or consequentially, from or related to any interim participation in Activity by the applicant and from the disapproval of the application to be a Customer is solely at the applicant's risk and expense, and this Corporation has no responsibility for any such damages, losses, costs, or liabilities.

1.5 Conditioned Participation

The Corporation may condition participation or continued participation in the Corporation on compliance by the Customer with special conditions, such as the establishment of escrow arrangements, the delivery of letters of credit, or other arrangements if the Corporation, in its sole discretion, determines such special conditions to be necessary or appropriate to avoid inordinate risk to the Corporation and other Customers.

1.6 Obligations, Rights and Responsibilities

1.6.1 Obligation to Become a Customer

Subject to Rule 1.4 of this rulebook, an entity that is eligible to be a Customer may not participate in Activity unless and until it becomes a Customer.

1.6.2 Right to Use the Mark

Each Customer may only use a Mark that the Customer is authorized to use pursuant to License by the Corporation.

1.6.3 Right to Connect Eligible POI Terminals

Customers, in accordance with the Rules, may connect to the Interchange System, through a Sponsoring Principal, an unlimited number of eligible POI Terminals (as defined in Chapter 7, "Acquiring," Rule 7.8), but only in the country or countries where the Corporation has expressly Licensed such Sponsoring Principal.

1.6.4 License Not Transferable

A Customer cannot transfer or assign its License, whether by sale, consolidation, merger, operation of law, or otherwise, without the express written consent of the Corporation, provided, however, that in the event that the Cards issued by, the Ownership of, or any Activity of a Customer are acquired by any person, whether by sale, consolidation, merger, operation of law or otherwise, the obligations, but not the rights, of such Customer shall transfer to the person acquiring such Customer.

1.6.5 Right to Sponsor Affiliates

A Principal has the right to Sponsor as an Affiliate any eligible entity, which is principally engaged in business in the same country as the Principal.

Upon application, the Corporation in its discretion may permit a Principal to Sponsor, as an Affiliate, an eligible entity which is principally engaged in business in another country, if the Corporation determines that such an arrangement will serve the best interests of the Corporation and is permissible under applicable laws.

1.6.5.1 Termination of Sponsorship

A Principal may terminate its Sponsorship of an Affiliate by giving the Corporation and the Affiliate at least six (6) months' prior written notice, unless the Corporation approves a shorter period.

Any other eligible Principal may subsequently Sponsor an Affiliate that is eligible for participation, and that has been terminated by its Sponsor.

1.6.6 Customer Responsibilities

Each Customer must:

1. At all times be entirely responsible for and Control all aspects of its Activities, and the establishment and enforcement of all management and operating policies applicable to its Activities, in accordance with the Standards;
2. Not transfer or assign any part or all of such responsibility and Control or in any way limit its responsibility or Control;
3. Ensure that all policies applicable to its Activities conform to the Standards and applicable law;
4. Conduct meaningful and ongoing monitoring to ensure compliance with all of the responsibilities set forth in this Rule;
5. Maintain a significant economic interest in each of its Activities; and
6. Operate Activities at a scale or volume of operations consistent with the business plan(s) approved by the Corporation in connection with the

application to be a Customer or application for a License, or both, as the case may be.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," of this rulebook.

1.7 Termination of License

A Customer License may terminate in one of two ways: voluntary termination and termination by the Corporation. Rights, liabilities and obligations of terminated Customers are set forth in Rule 1.7.4 of this rulebook.

NOTE

Additional regional Rules and Rules variations on this topic appear in Chapter 17, "Europe Region," of this rulebook.

1.7.1 Voluntary Termination

1.7.1.1 Principal

A Principal may voluntarily terminate its License.

In order to voluntarily terminate its License, the Customer must give written notice addressed to the Secretary of this Corporation by registered or certified mail, return receipt requested, or by personal or reputable courier service.

The notice must:

1. State that the notice is a notice of termination;
2. Be received by the Secretary;
3. Fix a date on which the termination will be effective, which must be at least one (1) year after the notice is received by the Secretary; and
4. Be otherwise in the form as may be required from time to time by the Corporation.

1.7.1.2 Affiliate

An Affiliate must give, through its Sponsoring Principal, at least six (6) months prior written notice to the Corporation of its intent to withdraw from participation in the Corporation unless the Corporation approves a shorter period.

A Principal that Sponsors a withdrawing Affiliate is responsible for notifying the Corporation of the Affiliate's compliance with the Rules.

1.7.2 Withdrawing a Cardbase from the Corporation

A Principal must not withdraw a Cardbase from the Corporation except upon fulfillment of the following conditions:

1. The Principal must provide the Corporation with at least six (6) months prior written notice of its intent to withdraw a Cardbase(s). If confidential negotiations surrounding a Cardbase sale would render six (6)-months' notice unduly disruptive, the Corporation may accept a shorter time at its discretion.
2. The Principal must certify in writing to the Corporation that on the intended date of withdrawal no card in circulation will bear the Marks, unless the Corporation has approved a plan for the phased withdrawal of the Cardbase. Any phased withdrawal must not exceed the lesser of one (1) full reissuance cycle or two (2) years. No plan will be acceptable to the Corporation unless it guarantees that such Cards still in circulation bearing Marks will continue to provide access to Accounts through the Corporation.
3. If there is a new owner of the Cardbase, such owner must be a Customer of the Corporation, at least during the phased withdrawal period. Alternatively, if the new owner is not eligible to be Licensed, then it must enter into an agreement with the Corporation to be bound by all Rules applicable to the Cardbase during its withdrawal period.
4. Any Issuer who withdraws from the Corporation must eradicate or disable all Corporation applications resident on Chip Cards that it has issued, within six (6) months after the effective date of its withdrawal. With respect to any such Card not used during the six (6) month period, the Issuer must block all the Corporation applications the first time the Card goes online.

1.7.3 Termination by the Corporation

A Customer's License may be terminated by the Corporation. The termination is effective upon delivery, or an inability to deliver after a reasonable attempt to do so, of written or actual notice by the Corporation to the Customer.

The Corporation may, at its sole discretion, effect such termination forthwith and without prior notice if:

1. The Customer suspends payments within the meaning of Article IV of the Uniform Commercial Code in effect at the time in the State of Delaware, regardless of whether, in fact, the Customer is subject to the provisions thereof; or
2. The Customer takes the required action by vote of its directors, stockholders, members, or other persons with the legal power to do so, or otherwise acts, to cease operations and to wind up the business of the Customer, such termination of License to be effective upon the date of the vote or other action; or
3. The Customer fails or refuses to make payments in the ordinary course of business or becomes insolvent, makes an assignment for the benefit of

creditors, or seeks the protection, by the filing of a petition or otherwise, of any bankruptcy or similar statute governing creditors' rights generally; or

4. The government or the governmental regulatory authority having jurisdiction over the Customer serves notice of intention to suspend or revoke, or suspends or revokes, the operations or the charter of the Customer; or
5. A liquidating agent, conservator, or receiver is appointed for the Customer, or the Customer is placed in liquidation by any appropriate governmental, regulatory, or judicial authority; or
6. The Customer's right to engage in Activity is suspended by the Corporation due to the Customer's failure to comply with the Corporation's AML Program or applicable law or regulation, and such suspension continues for twenty-six (26) consecutive weeks; or
7. A Customer fails to engage in Activity for twenty-six (26) consecutive weeks; or
8. The Customer is no longer Licensed to use the Marks.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," of this rulebook.

1.7.4 Liabilities and Obligations following Termination

A Customer who is terminated or who voluntarily withdraws its participation in the Corporation:

1. has no rights or privileges of participation in the Corporation after the effective date of termination, except as may be specifically provided in the Rules, and the regulations, policies, and technical specifications of the Corporation, or its License, in order to permit the orderly winding up of its affairs as a Customer;
2. is not entitled to a refund of any dues, fees, assessments or other payments. Such Customer remains liable for financial and other duties and obligations through the effective date of termination, and remains liable for any approved but uncollected assessments or expenses, relating to acts and events that occurred or that will have occurred during its term of participation or expenses that were incurred or will have been incurred during its term of participation;
3. must stop issuing Cards and distributing materials incorporating any Marks, on the date it gives notice that it is leaving the Corporation, or on the date it is given notice of termination;
4. must have replaced all Cards bearing any Marks, no later than the date of leaving the Corporation;
5. must remove any Marks from all POI Terminal locations on the date it leaves the Corporation;

6. must promptly return to the Corporation, all systems and confidential information that are proprietary to the Corporation and all materials displaying the Marks;
7. must immediately notify all its Cardholders of its termination and its effects on them, in accordance with the Rules;
8. must immediately send each of its Sponsored Affiliates notice, indicating how to obtain a new Sponsor to prevent such Affiliate's participation in the Corporation from terminating;
9. must continue to provide all necessary support for the Affiliates it Sponsors until the termination date;
10. remains liable to the Corporation and other Customers for the periods specified in the Rules, and its License, for Transactions arising, either before or after termination, from the use of any Card it, or its Sponsored Affiliates have issued, or from any of its POI Terminals connected, directly or indirectly, to the Interchange System.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," of this rulebook.

NOTE

Regional Rule variations on this topic appear in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number Rule Title	Category
1.1 Types of Customers	A
1.2 Eligibility to be a Customer	A
1.3 Application to be a Customer	A
1.4 Interim Participation	A
1.5 Conditioned Participation	A
1.6 Obligations, Rights and Responsibilities	A
1.7 Termination of License	A

Chapter 2 Licensing and Licensed Activities

This chapter contains information about licensing and rights and obligations related to Licensed Activity by Customers.

2.1 Purpose of License; Eligibility

Each Customer must execute a License in such form as is required by the Corporation. Each Customer must assist the Corporation in recording any License granted to the Customer if required in the country in which the Customer is Licensed or otherwise upon request of the Corporation. The Corporation may add additional requirements or limitations or other conditions to a License then in effect. In the event of an inconsistency between a Standard and a provision in a License, the Standard prevails and the License is deemed to be amended so as to be consistent with the Standard.

2.2 License Application

An application for a License must be made in the form and include all information then required. An applicant for a License must agree and, by execution and submission of an application for a License agrees, and by use of a Mark agrees, to comply with all provisions of the License pertaining to use of a Mark and with the Standards of this Corporation as may be in effect from time to time. A Licensee may not transfer or assign its License, whether by sale, consolidation, merger, operation of law, or otherwise without the express written consent of the Corporation; provided however, that in the event that the Cards issued by, the Ownership of, or any Activity of a Customer are acquired by any person, whether by sale, consolidation, merger, operation of law or otherwise, the obligations, but not the rights, of such Customer shall transfer to the person acquiring such Customer.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," of this rulebook.

2.2.1 Single European Payment Area License—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

2.2.2 *PayPass* License

NOTE

Rules on this topic appear in Chapter 21, "Maestro *PayPass*," of this rulebook.

2.3 Area of Use

Except as otherwise provided in the Standards, each Customer may use a Mark solely in the Area of Use in which the Customer has been granted a License. If the License does not specify an Area of Use, the License is deemed to authorize the Customer to use the Mark only in the country or countries the Corporation determines to be the Customer's Area of Use.

A License that the Corporation deems to be inconsistent with this Rule 2.3 is deemed amended effective as of the granting of the License so as to be consistent with this Rule.

Except as otherwise provided in the Standards, the BIN/IIN under which Cards are issued or acquired must accurately reflect the Area of Use in the corresponding License.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," of this rulebook.

2.3.1 Transaction Location

For the sole purpose of determining an Acquirer's Area of Use, a Transaction arising from a Point of Interaction (POI) Terminal with no fixed location (for example, a POI Terminal aboard a train or ship) takes place in the country where the Merchant is headquartered or where the Transaction is processed.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," of this rulebook.

2.3.2 Extending or Otherwise Modifying the Area of Use

A Customer must apply to the Corporation for permission to extend or otherwise modify the Area of Use of a License. Such application must be made in the form and include all information then required. If the application is approved, the Corporation will amend the License to reflect the change in the Area of Use.

Notwithstanding the foregoing, and with the exception of India, where conducting any of the following activities is prohibited without a license in India and written authorization from the Reserve Bank of India, a Customer is not required to make such application to conduct any of the following Activities, subject to (a) the Corporation's right to prohibit or restrict or condition any such Activity and (b) compliance by the Customer with Standards, laws and regulations applicable to any such Activity:

1. Issue Cards outside of the Area of Use, provided that the Customer does not use Solicitations or Solicit outside of the Area of Use.

2. Solicit and issue Cards to citizens of any country within the Area of Use, wherever such citizens reside. Any Card Solicitation, wherever conducted, must be directed only to residents of countries within the Customer's Area of Use.
3. Acquire Transactions from Merchants located in a country within the Area of Use, even if such Transactions arise from electronic commerce Transactions that the Merchant effects with Cardholders in countries outside of the Customer's licensed Area of Use.
4. Acquire electronic commerce Transactions, from Merchants located outside of the Customer's Area of Use, if such Transactions reflect sales to Cardholders residing within the Customer's Area of Use.
5. Acquire airline Transactions in a country outside of the Customer's Licensed Area of Use, subject to all of the following requirements:

    a. The airline has a meaningful presence in at least one country within the Area of Use; and

    b. The Customer identifies the airline Transactions as occurring in the Region in which the airline ticket office is located; and

    c. The Customer authorizes, clears, and settles each "local Transaction" in a manner that does not significantly disadvantage an Issuer in the same country in the judgment of the Corporation.

A Merchant's location generally is deemed to be the address set forth in the Merchant Agreement. The location of a Merchant conducting e-commerce Transactions may be determined based in full or in part on where the entity holds a License, pays taxes, or maintains an address for purposes of receiving mail. Any disagreement between Customers regarding a Merchant location may be referred to the Corporation for final resolution.

As used in this Rule 2.3.2, a "local Transaction" means a Transaction by a Cardholder residing in a country that takes place at a Merchant located in the same country.

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

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

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

2.3.3 Central Acquiring

NOTE

Regional Rules on this topic appears in Chapter 17, "Europe Region," of this rulebook.

2.4 MasterCard Anti-Money Laundering Program

A License application must be accompanied by affirmative evidence satisfactory to the Corporation that the applicant is in compliance with the MasterCard Anti-Money Laundering Program (the "AML Program"). Each Customer must, at all times, be in compliance with the AML Program.

The Corporation has exclusive authority to determine at any time whether an applicant or a Customer is in compliance with the AML Program. Each applicant to be a Customer and each Customer must cooperate with any effort by the Corporation to evaluate such applicant's or Customer's compliance with the AML Program. The Corporation may condition initial or continued License upon compliance with special conditions that the Corporation deems necessary or appropriate to ensure continued compliance with the AML Program by the applicant, Customer, and Corporation, as the case may be.

2.5 Obligations of a Sponsor

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

2.6 Name Change

The Corporation must receive written notice at least sixty (60) calendar days before the effective date of any proposed Customer name change. A Customer that proposes to change its name must promptly undertake necessary or appropriate action to ensure that its License(s) and Activities disclose the true identity of the Customer.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
2.1 Purpose of License; Eligibility	A
2.2 License Application	A
2.3 Area of Use	A
2.4 MasterCard Anti-Money Laundering Program	A
2.5 Obligations of a Sponsor	C
2.6 Name Change	C

Chapter 3 Customer Obligations

This chapter contains information about Customer obligations.

3.1 Standards

From time to time, the Corporation promulgates Standards governing the conduct of Customers and Activities. The Corporation has the right in its sole discretion to interpret and enforce the Standards. The Corporation has the right, but not the obligation, to resolve any dispute between or among Customers including, but not limited to, any dispute involving the Corporation, the Standards, or the Customers' respective Activities, and any such resolution by the Corporation is final and not subject to appeal or other reviews. In resolving disputes between or among Customers, or in applying its Standards to Customers, the Corporation may deviate from any process in the Standards or that the Corporation otherwise applies, and may implement an alternative process, if an event, including, without limitation, an account data compromise event, is, in the sole judgment of the Corporation, of sufficient scope, complexity and/or magnitude to warrant such deviation. The Corporation will exercise its discretion to deviate from its Standards only in circumstances the Corporation determines to be extraordinary. Any decision to alter or suspend the application of any process(es) will not be subject to review or other challenge. The Corporation reserves the right to limit, suspend or terminate a Customer's License, if that Customer does not comply with any Standards or with any decision of the Corporation with regard to the interpretation and enforcement of any Standard, or that in any respect violates any Standard or applicable law.

This rulebook contains the Rules applicable to interregional, intraregional and domestic activity, unless an approved published regional or domestic Rule exists. Regional and Maestro *PayPass* Rule variations are indicated and appear in full text in the applicable regional or Maestro *PayPass* chapter of this rulebook. The Rules apply to Maestro POS and ATM Transactions and to Debit MasterCard PIN POS Transactions.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

3.1.1 Variances

A variance is the consent by the Corporation for a Customer to act other than in accordance with a Standard. Only a Customer may request a variance. Any such request must specify the Rule(s) or other Standard(s) for which a variance is sought. To request a variance, a Customer must submit to the Corporation a completed Variance Request Form (Form 759), available on MasterCard Connect.

If the Customer claims to be prevented from fully complying with a Standard because of law or regulation, the Customer must provide a copy of the law or regulation and if such law or regulation is in a language other than English, a complete certified English translation. As a condition of granting a variance for that reason, the Corporation may require the Customer to undertake some other form of permissible Activity.

The Corporation may assess a fee to consider and act on a variance request.

3.1.2 Failure to Comply with a Standard

Failure to comply with any Standard(s) adversely affects the Corporation and its Customers and undermines the integrity of the MasterCard system. Accordingly, a Customer that fails to comply with any Standard is subject to assessments ("noncompliance assessments") as set forth in the Standards. In lieu of or in addition to the imposition of a noncompliance assessment, the Corporation, in its sole discretion, may require a Customer to take such action and the Corporation itself may take such action as the Corporation deems necessary or appropriate to ensure compliance with the Standards and safeguard the integrity of the MasterCard system. In the exercise of such discretion, the Corporation may consider the nature, willfulness, number and frequency of occurrences and possible consequences resulting from a failure to comply with any Standard(s). The Corporation may provide notice and limited time to cure such noncompliance before imposing a noncompliance assessment.

3.1.2.1 Noncompliance Categories

The Corporation has implemented a compliance framework designed to group noncompliance with the Standards into three (3) categories.

3.1.2.1.1 Category A—Payment System Integrity

Category A noncompliance affects payment system integrity. The Corporation has the authority to impose monetary noncompliance assessments for Category A noncompliance with the Standards. "Payment system integrity" violations include, but are not limited to, noncompliance involving License requirements, Merchant signing and monitoring requirements, ATM owner signing and monitoring requirements, or protection of Card, account, or Transaction information.

3.1.2.1.2 Category B—Visible to Customers

Category B noncompliance addresses conduct that is visible to customers. The Corporation has the authority to impose monetary noncompliance assessments for Category B noncompliance or, in the alternative, may provide notice and a limited time to cure such noncompliance before imposing monetary assessments. "Visible to customers" violations include, but are not limited to, noncompliance involving the use of the Marks, identification of the Merchant at the point of interaction, the setting of minimum and maximum Transaction amounts, the payment of Merchants and Sub-merchants for Transactions, POI Terminal Transaction receipt requirements, and ATM access fee notices.

3.1.2.1.3 Category C—Efficiency and Operational Performance

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

3.1.2.2 Noncompliance Assessments

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

Noncompliance Category	Assessment Type	Assessment Description
A	Per Violation	First violation: up to USD 25,000 Second violation within 12 months: up to USD 50,000 Third violation within 12 months: up to USD 75,000 Fourth and subsequent violations within 12 months: Up to USD 100,000 per violation
	Variable Occurrence(by device or Transaction)	Up to USD 2,500 per occurrence for the first 30 days Up to USD 5,000 per occurrence for days 31–60 Up to USD 10,000 per occurrence for days 61–90 Up to USD 20,000 per occurrence for subsequent violations
	Variable Occurrence(by number of Cards)	Up to USD 0.50 per card Minimum USD 1,000 per month per Cardbase No maximum per month per Cardbase No maximum per month per Cardbase or per all Cardbases
B	Per Violation	First violation: up to USD 20,000 Second violation within 12 months: up to USD 30,000 Third violation within 12 months: up to USD 60,000 Fourth and subsequent violations within 12 months: Up to USD 100,000 per violation

Noncompliance Category	Assessment Type	Assessment Description
	Variable Occurrence(by device or Transaction)	Up to USD 1,000 per occurrence for 30 days Up to USD 2,000 per occurrence for 31–60 days Up to USD 4,000 per occurrence for 61–90 days Up to USD 8,000 per occurrence for subsequent violations
	Variable Occurrence(by number of Cards)	Up to USD 0.30 per Card Minimum USD 1,000 per month per Cardbase Maximum USD 20,000 per month per Cardbase Maximum USD 40,000 per month per all Cardbases
C	Per Violation	First violation: up to USD 15,000 Second violation within 12 months: up to USD 25,000 Third violation within 12 months: up to USD 50,000 Fourth and subsequent violation(s) within 12 months: up to USD 75,000 per violation
	Variable Occurrence(by device or Transaction)	Up to USD 1,000 per occurrence for the first 30 days Up to USD 2,000 per occurrence for days 31–60 Up to USD 4,000 per occurrence for day Up to USD 8,000 per occurrence for subsequent violations
	Variable Occurrence(by number of Cards)	Up to USD 0.15 per card Minimum USD 1,000 per month per Cardbase Maximum USD 10,000 per month per Cardbase Maximum USD 20,000 per month per all Cardbases

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

3.1.2.3 Certification

A senior executive officer of each Principal must, if requested by the Corporation, promptly certify in writing to the Corporation the status of compliance or noncompliance with any Standard by the Customer or by any of such Customer's Sponsored Affiliates.

3.1.2.4 Review Process

A Customer may request that the Secretary of this Corporation review an assessment imposed by the Corporation for noncompliance with a Standard. Such a request must be submitted in writing and signed by the Customer's principal contact. The request must be postmarked no later than 30 calendar days after the date of the disputed assessment.

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

3.1.2.5 Resolution of Review Request

When a Customer requests review of an assessment for noncompliance with a Standard, the Secretary of this Corporation may take such action as he or she deems necessary or appropriate or may elect not to act. The Secretary may delegate authority to act or not to act with respect to any particular matter or type of matter. If the Secretary or his or her designee elects to conduct further inquiry into the matter, each Customer must cooperate promptly and fully. If the Secretary or his or her designee makes a recommendation of action to resolve the matter, such recommendation is final and not subject to further review or other action.

3.1.3 Rules Applicable to Intracountry Transactions

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

3.1.4 Communication of Intracountry Fallback Rules

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

3.2 Conduct of Activity

Each Customer at all times must conduct Activity in compliance with the Standards and with all applicable laws and regulations. Each Customer must conduct all Activity and otherwise operate in a manner that is financially sound and so as to avoid risk to the Corporation and to other Customers.

3.2.1 Conflict with Law

A Customer is not required to undertake any act that is unambiguously prohibited by applicable law or regulation.

3.2.2 Obligations of a Sponsor

Each Principal that Sponsors one or more Affiliate must cause each such Affiliate to comply with all Standards applicable to the Activity of that Affiliate. A Principal is liable to the Corporation and to all other Customers for all Activities of any Affiliate Sponsored by the Principal and for any failure by such Sponsored Affiliate to comply with a Standard or with applicable law or regulation.

If an Affiliate Sponsored by a Principal ceases to be so Sponsored by that Principal, such Principal nonetheless is obligated, pursuant to and in accordance with the Standards, to acquire from other Customers the records of Transactions arising from the use of Cards issued by that formerly Sponsored Affiliate and whether such Transactions arise before or after the cessation of the Sponsorship.

3.2.3 Affiliates

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

- Action taken by such Affiliate to satisfy such liability or obligation with, through or by a Principal that Sponsors or Sponsored such Affiliate, or
- Agreement between any Principal and such Affiliate.

In accordance with the Standards and in compliance with applicable laws and regulations, each Principal will have access to and may use or otherwise process its Sponsored Affiliates' confidential information and Confidential Transaction Data (as defined in Rule 3.7.2 of this rulebook) in connection with authorization, settlement, clearing, fraud reporting, chargebacks, billing, and other related activities.

3.2.4 Compliance

From time to time, the Corporation may develop means and apply criteria to evaluate a Customer's compliance with Rule 3.2 of these Rules. Each Customer must promptly provide in writing any information requested by the Corporation and must fully cooperate with any effort by the Corporation and the Corporation's representatives to evaluate a Customer's compliance with Rule 3.2.

In the event that the Corporation determines that a Customer is not complying or may not on an ongoing basis comply with the requirements of Rule 3.2 of this rulebook, the Corporation may:

1. Impose special terms upon the Customer as the Corporation deems necessary or appropriate until each condition or discrepancy is resolved to the Corporation's satisfaction so as to enable the Customer to be and to remain in full compliance with Rule 3.2 of this rulebook, or
2. Require the Customer to withdraw its License.

3.3 Choice of Laws

The substantive laws of the State of New York govern all disputes involving the Corporation, the Standards, and/or the Customers and Activity without regard to conflicts. Any action initiated by a Customer regarding and/or involving the Corporation, the Standards and/or any Customer and Activity must be brought, if at all, only in the United States District Court for the Southern District of New York or the New York Supreme Court for the county of Westchester, and any Customer involved in an action hereby submits to the jurisdiction of such courts and waives any claim of lack of personal jurisdiction, improper venue, and *forum non conveniens*.

This provision in no way limits or otherwise impacts the Corporation's authority described in Rule 3.1 of this rulebook. Each Customer agrees that the Standards are construed under, and governed by, the substantive laws of the State of New York without regard to conflicts.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

3.4 Examination and Audits

The Corporation reserves the right to conduct an audit or examination of any Customer and Customer information to ensure full compliance with the Standards of the Corporation. Any such audit or examination is at the expense of the Customer, and a copy of the audit or examination results must be provided promptly to the Corporation upon request.

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

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

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

3.5 Temporary Suspension of Services and Participation

In the event of an emergency, which in the opinion of the Corporation poses a threat to the safety and soundness of the Corporation, including but not limited to its security, financial or operational integrity, the Corporation may temporarily suspend any Corporation services, or the participation of any entity in any such services.

3.6 Non-discrimination

3.6.1 POS Transactions

Customers may not discriminate against any Merchant with regard to processing and authorizing Transactions received.

3.6.2 Terminal Transactions

Pursuant to the Rules, and the regulations, policies and technical specifications of the Corporation, each Customer must:

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

Except as permitted under the Rules, a Customer must not discriminate against other Customers of the Corporation as to any of the terms or conditions upon which it honors Cards, or MasterCard cards, or acquires or processes Transactions or MasterCard transactions.

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

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

3.7 Provision and Use of Information

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and Chapter 20, "United States Region" of this rulebook.

3.7.1 Obligation of a Customer to Provide Information

Upon request by the Corporation, and subject to applicable law or regulation, a Customer must provide Customer Reports to the Corporation, or to the Corporation's designee: provided, compliance with the foregoing obligation does not require a Customer to furnish any information, the disclosure of which in the opinion of this Corporation's legal counsel, is likely to create a significant potential legal risk to this Corporation and/or its Customer(s). To the extent that a Customer is obligated to provide a Customer Report to the Corporation that the Customer deems to disclose proprietary information of the Customer, such information will be treated by the Corporation with the degree of care deemed appropriate by the Corporation to maintain its confidentiality.

As an example of a Customer Report, each Acquirer must provide Transaction Data to the Corporation in such form and manner as the Corporation may require. As used herein, "Transaction Data" means any data and or data element or subelement that the Standards require to be used to process or settle a Transaction (whether processed and/or settle via the Interchange System or otherwise) or that the Corporation requires to be provided.

3.7.2 Confidential Information of Customers

A Customer must provide Confidential Transaction Data to the Corporation or through the Corporation's processes or systems solely as prescribed by the Standards or as otherwise required by the Corporation or applicable law. For example, a primary account number (PAN) must not be provided through the Interchange System except as required by the technical specifications or other Standards pertaining to the Interchange System or a component thereof.

The Corporation and its parents, subsidiaries and affiliates (herein collectively referred to as the "Corporation's Affiliates") will not use or disclose confidential information or Confidential Transaction Data furnished to it by Customers or Merchants except to the extent that the use or disclosure is in compliance with applicable law and as specifically provided herein. "Confidential Transaction Data" means any information provided to the Corporation or any of the Corporation's Affiliates by a Customer or Merchant if that information enables the Corporation or any of the Corporation's Affiliates to determine an individual's identity or includes an Account number. The Corporation may use and/or disclose confidential information and Confidential Transaction Data only as follows:

1. for the benefit of the Customer supplying the information to support the Customer's Program and/or Activities;

2. as may be appropriate to the Corporation's and the Corporation's Affiliates' staff, accountants, auditors, or counsel;
3. as may be required or requested by any judicial process or governmental agency having or claiming jurisdiction over the Corporation or the Corporation's Affiliates;
4. as required for processing Transactions, including authorization, clearing, and settlement Activities;
5. for accounting, auditing, billing, reconciliation, and collection activities;
6. for the purpose of processing and/or resolving chargebacks or other disputes;
7. for the purpose of protecting against or preventing actual or potential fraud, unauthorized Transactions, claims, or other liability, including to third parties providing these services;
8. for the purpose of managing risk exposures, franchise quality, and compliance with Rules and the Standards;
9. for the purpose of providing products or services to Customers or other third parties, except that any Confidential Transaction Data provided in such products or services will only be provided to a Customer and will consist solely of Confidential Transaction Data provided to the Corporation or any of the Corporation's Affiliates by that Customer;
10. for the purpose of administering sweepstakes, contests, or other promotions;
11. for preparing internal reports for use by the Corporation or any of the Corporation's Affiliates, staff, management, and consultants in operating, evaluating, and managing Corporation business;
12. for preparing and furnishing compilations, analyses, and other reports of aggregated information, and anonymizing confidential information and/or Confidential Transaction Data, provided that such compilations, analyses, or other reports do not identify any (i) Customer other than the Customer for which the Corporation or any of the Corporation's Affiliates prepares the compilation, analysis, or other report or (ii) Cardholder whose Transactions were involved in the preparation of the compilations, analysis, or other report;
13. for the purpose of complying with applicable legal requirements; or
14. for other purposes for which consent has been provided by the individual to whom the confidential information and/or Confidential Transaction Data relates.

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

3.7.3 Use of Corporation Information by a Customer

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

NOTE

Additional regional Rules on this topic appear in Chapter 20, "United States Region" of this rulebook.

3.7.4 Confidential Information of the Corporation and the Corporation's Affiliates

A Customer must not disclose confidential information of the Corporation or of the Corporation's parents, subsidiaries, and Affiliates (herein collectively referred to as the "Corporation's Affiliates") except:

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

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

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

3.8 Record Retention

During the term of participation and for two (2) years after termination of participation, each Customer agrees to receive and hold in confidence any and all materials or information considered proprietary or confidential by any other Customer.

For the purposes of this section of the Rules, confidential information includes, without limitation, the following:

1. information concerning technical practices in implementing and operating the Corporation;
2. information concerning the entity under consideration for a License from the Corporation, prior to public disclosure;
3. Transaction volume and any other statistical information relating to the operation of the Corporation;
4. Identity Standards;
5. information concerning applications, specifications, Licenses, operating systems, and value-added data on Chip Cards.

Customers must retain records of Transactions communicated to, or by it, or on behalf of, 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 17, "Europe Region," of this rulebook.

3.9 Cooperation

Customers must fully cooperate with the Corporation and all other Customers in the resolution of Cardholder and settlement disputes.

Customers to the best of their ability must provide requested investigative assistance to any other Customer.

Customers that receive a request for investigative assistance must acknowledge receipt of the request within five (5) business days of receipt.

Customers performing investigative services at the request of another Customer are entitled to payment for such services, at a rate and total cost that is previously agreed to by both parties.

3.9.1 Fraudulent or Suspicious Transactions

Customers may request information from any other Customer regarding fraudulent or suspicious Transactions.

3.9.2 Photographs

Customers may request copies of photographs taken with surveillance cameras. The Acquirer must provide the Customer requesting photographs a written cost proposal that must be accepted by the requesting Customer before production of the photographs. The Acquirer is entitled to recover the actual expenses associated with supplying such photographs.

3.10 Quarterly MasterCard Reporting (QMR)

Each Customer must complete and timely deliver to the Corporation the Quarterly MasterCard Report or such other Customer Report as the Corporation may require be completed and returned by Customers from time to time (such Customer Report being hereinafter referred to as the "QMR") in the manner and at such time as the corporation requires.

3.10.1 Report Not Received

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

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

3.10.2 Erroneous or Incomplete

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

1. Impose on the Customer, after review of the Customer's previously correctly submitted QMR and assessments paid thereon an assessment equal to, or

greater than, the Customer's last properly paid assessment for each calendar quarter for which it submitted an erroneous or incomplete QMR;

2. Impose on the Customer a noncompliance assessment, as set forth in the applicable regional *MasterCard Consolidated Billing System* manual;
3. If the Corporation's estimate of payment due results in an underpayment by the Customer, collect the amount of the underpayment due and impose on the Customer an assessment on the amount of the underpayment of the lower of two (2) percent per month or the highest rate permitted by law, from the date(s) the payment(s) was first due and payable through the date(s) on which the additional amounts(s) due is paid;
4. If the Corporation's estimate of payment due results in an overpayment by the Customer, return the amount of the overpayment, without penalty or interest thereon, as soon as practicable after the overpayment amount is identified and calculated; and
5. Collect of the assessment amount, and any interest, from the Customer's settlement account.

3.10.3 Overpayment Claim

If a Customer, after submitting a QMR, submits to the Corporation a claim asserting an overpayment thereon, the Corporation may:

1. Accept the claim for review only if it is received by the Corporation no later than one calendar quarter after the date of the claimed overpayment; and
2. Provided the overpayment claim is submitted in a timely manner and substantiated, return the amount of the overpayment to the Customer, without interest or penalty thereon, as soon as practicable after the overpayment amount is identified and calculated.

A Customer may request the Corporation's Secretary review the Corporation's actions and make a finding or recommendation. Such a request must be received by the Secretary no later than 30 calendar days after the date of the disputed action and any finding or recommendation by the Secretary with regard to the matter will be final and not subject to appeal or other similar action.

3.11 Card Fees and Reporting Procedures

3.11.1 Card Fees

A Principal must pay fees based upon the number of Cards that they Sponsor in the Corporation. Such fees are payable in accordance with and subject to appropriate provisions of the Rules, Standards and applicable agreements.

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

3.11.2 Card Count Reporting Procedures

On or before 30 September of each year, the Corporation will deliver listings to Principals of each specific IIN, which appears on the Corporation's routing tables for each Affiliate. On or before 31 October of each year, Principals must certify a count of the number of Cards that are issued using a specific IIN, which appears on the report provided by the Corporation. Alternatively, Principals must certify a count of the number of Accounts, which have Cards issued for access using a specific IIN, which appear on the report provided by the Corporation. Principals must confirm in writing to the Corporation, their certification and the certifications of their Affiliates. When a count of the number of Accounts which have Cards issued for access is provided, the Corporation will multiply the number provided by a factor of one and four tenths (1.4) to determine the number of Cards issued.

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

3.12 Contact Information

Each Principal must provide the Corporation with up-to-date mailing addresses, air express/hand delivery addresses, telephone numbers, fax, and telex addresses (when available), whenever contact information changes.

3.13 Safeguard Card Account and Transaction Information

Each Customer, for itself and any third party that may be afforded access to Transaction or Card account information, or both, by or on behalf of the Customer, must safeguard and use or permit use of such information in accordance with the Standards

3.14 Satisfaction of Minimum Financial Requirements

Each Customer at all times must satisfy the minimum financial requirements established by the Corporation from time to time. The Corporation, in its discretion, may establish different or additional financial requirements for:

1. A category of financial institutions, Corporations, or corporations or other entities that are eligible to become a Customer, or
2. An individual Customer or prospective Customer in the manner set forth in the Standards should the Corporation determine that different or additional requirements are reasonably appropriate to evidence the financial integrity of a type of Customer or an individual Customer or prospective Customer.

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

3.15 Integrity of Brand and Network

A Customer may not directly or indirectly engage in or facilitate any action that is illegal, or that, in the judgment of the Corporation and whether or not addressed elsewhere in the Standards, damages or may damage the goodwill or reputation of the Corporation or of any Mark, and the Customer will promptly cease engaging in or facilitating any such action upon request of the Corporation.

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

NOTE

Additional regional Rules on this topic appear in Chapter 20, "United States Region," of this rulebook.

3.16 Transaction Requirements

Each Customer must, in accordance with the Standards:

1. Accept and present to the Issuer records of Transactions arising from the use of a Card issued by any other Customer from any Merchant the Customer has authorized to honor Cards;
2. Accept Transactions received from another Customer arising from the use of any Card issued by it;
3. Maintain, directly or indirectly, a functional twenty-four-hour per day operating connection to the Interchange System, and not force any other Customer wishing to operate multilaterally using the Interchange System into bilateral agreements.

3.17 Agreements between Customers

The rights, duties, obligations and limitations contained in the Rules, and the regulations, policies, License and technical specifications of the Corporation, apply to all Customers, except as they may be expressly limited by contract with the Corporation.

An Affiliate and its Sponsoring Principal may make other agreements or arrangements governing their relationships (including such matters as fees), providing these agreements or arrangements comply with the paragraph above.

3.18 Expenses of Customers

Each Customer is responsible for all the expenses they incur to comply with the Rules, and the regulations, policies and technical specifications of the Corporation, including, but not limited to computer hardware and software modifications, establishing and maintaining communication lines between a Processor and the Interchange System, and between each POI Terminal and its data processing facility. Nothing contained in this section limits the freedom of each Principal and Affiliate to negotiate the terms and conditions of their Sponsorship or License.

3.19 Fees, Expenses and Other Payment Obligations

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

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

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

Each Customer expressly authorizes the Corporation to take the Customer's funds and other assets as authorized by this Rule, and to apply such funds and other assets to any obligation of the Customer to the Corporation or any other person under the Standards, and no Customer shall have any claim against the Corporation or any other person in respect of such conduct by the Corporation. Each Customer agrees upon demand to promptly execute, acknowledge and deliver to the Corporation such instruments, agreements, lien waivers, releases, and other documents as the Corporation may, from time to time, request in order to exercise its rights under this Rule.

If the Corporation draws on the Customer's funds, the Corporation is not required to reimburse the Customer or any third party (including another Customer) for funds drawn which are owned by any of them or otherwise subject to any of their rights. The Customer and any third party (including another Customer) bear all risk and liability related to the funds drawn and shall jointly and severally indemnify and hold the Corporation harmless from all liability and claims arising from any such draw of funds.

3.19.1 Taxes and Other Charges

Each Customer must pay when due all taxes charged by any country or other jurisdiction in which the Customer conducts Activity with respect to such Activity. In the event the Corporation is charged taxes or other charges by a country or other jurisdiction as a result of or otherwise directly or indirectly attributable to Activity, the Customer is obligated to reimburse the Corporation the amount of such taxes or other charges and the Corporation may collect such taxes or other charges from the settlement account of the Principal responsible in accordance with the Standards for the Activity that gave rise to the charge.

3.20 Transaction Currency Information

Each Acquirer must inform the Corporation whether or not it submits Transactions in a currency which is not the official currency of the country where the Transactions took place, including Transactions on which POI currency conversion has been performed. This information must be provided annually and will include Merchant and Service Provider and any other information required to be reported. When there is a change in the currency(ies) in which Transactions are submitted, in relation to the Acquirer itself or a Merchant, or in the use of a Service Provider, the Acquirer is required to update its reported information no later than 30 days after the change.

3.21 Additional Obligations

Customers must:

1. actively promote the Corporation and its programs;
2. promptly pay to the Corporation all fees, assessments and other obligations when due; and
3. act in good faith and exercise due care when discharging their duties, obligations and responsibilities, and performing any act authorized or required pursuant to the Rules, and the regulations, policies and technical specifications of the Corporation.

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

3.22 Data Protection—Europe Region Only

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
3.1.2.3 Certification	C
3.2 Conduct of Activity	A
3.4 Examination and Audits	
3.6 Non-discrimination	A
3.7.1 Obligation of a Customer to Provide Information	C
3.7.4 Confidential Information of the Corporation and the Corporation's Affiliates	A
3.8 Record Retention	A
3.9 Cooperation	A
3.10 Quarterly MasterCard Reporting (QMR)	A
3.11 Card Fees and Reporting Procedures	C
3.12 Contact Information	C
3.13 Safeguard Card Account and Transaction Information	A
3.14 Satisfaction of Minimum Financial Requirements	A
3.15 Integrity of Brand and Network	A
3.16 Transaction Requirements	A
3.19.1 Taxes and Other Charges	C
3.20 Transaction Currency Information	C
3.21 Additional Obligations	A

Chapter 4 Marks

This chapter contains information about use of the Marks and competing marks.

4.1 Right to Use the Marks

A right to use one or more Marks is granted to Customers and other Licensees only pursuant to the terms of a License or other agreement with the Corporation. Unless an interim License has been granted, a Mark must not be used in any form or manner before the execution of a written License and, if applicable, a License addendum.

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

Except as otherwise set forth in Rule 1.6.4 of this rulebook, each License is non-exclusive and non-transferable. The right to use a Mark may be sublicensed by a Licensee to any Sub-licensee only in accordance with the Standards or otherwise with the express written consent of the Corporation. A Customer or other Licensee that is permitted to sublicense the use of a Mark to a Sub-licensee must ensure, for so long as the sublicense is in effect, that the Mark is used by the Sub-licensee in accordance with the Standards and/or other additional conditions for such use required by the Corporation.

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

A Customer must use the Marks in the manner prescribed in the License, the Standards, and the Identity Standards for all applications, including, but not limited to, uses on Cards, POI Terminals, signage, correspondence, and advertising.

A Customer may use the Marks as a stand-alone, incremental or cross-border brand for its Cardholders, at the discretion of the Corporation.

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

NOTE

Additional regional Rules on this topic appear in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

4.2 Protection and Registration of the Marks

Protection of the Marks is vital to the Corporation, its Customers and other Licensees. Any use of a Mark must not degrade, devalue, denigrate, or cause injury or damage to the Marks or the Corporation in any way.

By using any Mark, each Customer and other Licensee acknowledges that the Corporation has adopted, and is the exclusive owner, licensee, or both of certain marks and may in the future become the exclusive owner, licensee, or both of other marks that are or will be used by Licensees for the identification and promotion of the Corporation, which include Marks, as such term is defined in the Rules. All property rights in such marks and designations belong exclusively to the Corporation. All use of any Mark will inure solely to the benefit of the Corporation.

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

Without limitation, the foregoing shall specifically apply to registration or use of any mark or term that incorporates, references or otherwise could be confused or associated with a Mark currently or previously Licensed or otherwise used by a Customer (including, without limitation, by virtue of acquisition by merger or otherwise, bankruptcy or voluntary or involuntary winding-up).

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

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

A Customer must not threaten or initiate any litigation relating to the Marks and such other marks, without first obtaining the consent of the Corporation.

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

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," Chapter 17, "Europe Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook.

4.3 Misuse of a Mark

Each Customer and other Licensee must promptly notify the Corporation promptly, whenever it learns of any misuse of the any Marks, or of any attempt to copy or infringe the Marks or any portion thereof.

4.4 Review of Solicitations

The Corporation reserves the right to review samples and approve or refuse to approve use of a Solicitation. Amended samples, if required as a result of this review, also must be forwarded to the Corporation for review.

4.5 Display on Cards

A Customer that allows any of its Cardbases access to the Corporation must begin issuing Cards in compliance with the Identity Standards within nine (9) months and must be in full compliance within thirty-six (36) months of the date that the Cardbase(s) first had access to the Corporation.

The Marks may be placed on cards in combination with other local/regional POS debit mark and/or local/international ATM mark.

The Marks may co-reside on a Debit MasterCard card.

The Marks may not be placed on any:

1. debit card that does not qualify as a Card; or
2. credit card.

Customers must not place any other Competing EFT POS Network debit marks on their participating Cards. The Corporation may decide at its option to extend this prohibition to individual institutions, for all their Cards.

Acceptance of cards not bearing the Service Marks cannot be guaranteed.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," and Chapter 16, "Canada Region," and additional regional Rules and regional Rule Variations on this topic appear in Chapter 17, "Europe Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook.

4.5.1 Maestro *PayPass* Identifier on a Mobile Payment Device

The Maestro *PayPass* identifier must be displayed each time the account is accessed.

The Maestro *PayPass* identifier may co-reside in the same user interface as local/regional POS debit marks, any MasterCard Marks, and/or competing debit and credit marks, subject to the following:

1. The Maestro *PayPass* identifier must be given at least equal prominence.
2. The Maestro *PayPass* identifier must be at least as large as the marks of any competing debit and credit marks.

4.6 Display of the Marks at POI Terminals

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

A Customer must display the Marks in accordance with the Rules, and the regulations, policies and Identity Standards of the Corporation as may be published from time to time, within thirty (30) calendar days of the POI Terminal's first Transaction.

A Customer must not display signage in a false, deceptive or misleading manner.

All signage used by a Customer with respect to the Marks must comply with all applicable laws, Rules, and the regulations, policies, and Identity Standards of the Corporation.

The Marks may not be placed on or near, or otherwise used to identify any POS Terminal, which does not accept Cards.

The Corporation may permit or prohibit the display of the logo of a Competing EFT POS Network at POS Terminals.

4.6.1 New and Replacement Signage

All new and replacement signage, other than signage used to comply with Rule 4.5 of this rulebook, referring to POI Terminals that participate in the Corporation must comply with this Rule 4.6.1. On any new or replacement signage incorporating the marks of a competing network, the corresponding Marks must appear and be given at least equal prominence. The Marks must be at least as large as the marks of any competing network.

4.6.2 ATM Signage System

The MasterCard, Maestro, and Cirrus brands must be displayed on an ATM. 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, Maestro, Cirrus.

4.7 Digital Wallets

Third-party wallet developers must enter into a License agreement with the Corporation in order to use the Marks.

4.7.1 Global Minimum Branding Requirements

1. The Marks must appear where the account number appears in a digital wallet. Alternatively, an image of a generic Maestro® Card may be used to satisfy this requirement. A generic Card contains no Issuer or co-brander identification and must contain the Maestro Word Mark in the Issuer identification area. In all cases, the Cardholder must be able to discern clearly the Marks.

   When displaying a Card image, digital wallet developers must comply with all Identity Standards and the depiction of Cards in all Cardholder communications. This requirement includes the following provisions:

   a. digital wallet developers must make the Marks completely visible; and

   b. digital wallet developers must not distort or obscure the Marks in any way.

2. The placement and position of the Marks or the Card image must be close in proximity to the account number to make clear their association.

3. Digital wallet developers must use the Color Version in Match Colors of the Marks. The background screen colors must provide sufficient contrast to ensure that the Marks are clearly visible.

   If the wallet user can change the background colors of the wallet screens, the wallet developer must use the acceptance version of the Marks. The acceptance version is the color version in Match Colors with the Drop Shadow within the MasterCard Dark Blue Acceptance Rectangle.

4. Wallet developers must obtain the authorized Marks artwork from the MasterCard Brand Center Web site: www.mastercardbrandcenter.com

   Digital wallet developers must ensure that the images of the Marks comply with the Corporation's reproduction standards. Reproduction artwork for print media also is available from the Brand Center link.

5. Digital wallet developers must maintain parity when depicting the Marks with other acceptance marks in digital wallets. The Marks must be at least as prominent as, and appear in at least the same size and frequency as, all other acceptance marks displayed.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
4.1 Right to Use the Marks	A
4.2 Protection and Registration of the Marks	B
4.3 Misuse of a Mark	B
4.5 Display on Cards	B
4.6 Display of the Marks at POI Terminals	B

Chapter 5 Special Issuer Programs

This chapter contains information about Special Issuer Programs.

5.1 Special Issuer Programs—General Requirements

The Rules set forth in this Chapter 5 apply to Special Issuer Programs that the Corporation may identify as such from time to time.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

5.1.1 Prior Consent of the Corporation

A Customer may not conduct a Special Issuer Program without the express prior written consent of the Corporation and each Customer must operate each Special Issuer Program in accordance with the Standards as may be in effect at any given time. A Special Issuer Program name and Special Issuer Program Card design must be reviewed and approved by the Corporation in accordance with the Standards.

A request for approval must be submitted to the Corporation via the Special Issuer Program registration process. Registration forms, which are available to Issuers or their designated agents on MasterCard Connect, must include a detailed description of the Card Program.

5.1.2 Reservation of Rights

The Corporation reserves the right:

1. To approve or reject any Special Issuer Program application; and
2. To require that any previously approved Special Issuer Program be modified; and
3. To withdraw its approval of any Special Issuer Program and require the Special Issuer Program to be wound up and terminated.

A Customer may request that the Corporation's Secretary review the rejection or withdrawal of the approval of a Special Issuer Program by written request to the Corporation's Secretary within 30 days of receipt of the notice of rejection or withdrawal of approval. Any decision by the Corporation's Secretary with respect to such termination is final and not appealable.

5.1.3 Cardholder Communication

A Customer is required to provide each Cardholder offered a Card to be issued as part of a Special Issuer Program with the terms and conditions of the Special Issuer Program.

The Corporation determines whether any Cardholder Communication, including, by way of example and not limitation, a Solicitation, disclosure or other information about a Special Issuer Program, is satisfactory and in compliance with the Standards. As a condition of the commencement or continuation of a Special Issuer Program, the Customer must comply with the Corporation's Cardholder Communication requirements.

5.2 Affinity and Co-Brand (A/CB) Card Programs

5.2.1 Compliance with the Standards

Each Customer must operate A/CB programs in accordance with the Standards as may be in effect from time to time.

5.2.2 Program Approval

The Corporation must approve, in writing and in advance of the program launch, each A/CB program name and Card design.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

5.2.3 Ownership and Control of A/CB Programs

Ownership and Control of any A/CB program must reside with the Customer at all times. No arrangement is permitted that would enable the A/CB partner or any person or entity other than a Customer effectively to own or Control an A/CB program.

The Corporation, in its sole discretion, determines if an A/CB program is owned and Controlled by the Customer. The determination is based upon the Customer's entire relationship with the A/CB partner, not any one component. Factors considered include, but are not limited to:

1. whether the Customer establishes the program policies and guidelines, such as making Cardholder credit and eligibility decisions;
2. the Customer's role in setting the fees and rates for all benefits relating to the A/CB program provided to the Cardholder;
3. what the Customer has at risk;
4. whether the Customer actively ensures that its program policies and guidelines are being implemented;
5. the extent of ownership or Control of A/CB program receivables, whether all or a substantial part of the receivables are financed with the A/CB partner; and

6. the extent to which the Customer, and not the A/CB partner, is portrayed as the owner of the A/CB program.

5.2.4 Ownership of Receivables

An A/CB partner is prohibited from owning or Controlling A/CB program receivables. However, the assignment of receivables or sale of a participation in receivables to the A/CB partner, or some other financing vehicle involving the A/CB partner, is permitted if the program is owned and Controlled by the Customer.

5.2.5 Violation of A/CB Rules

If the Customer or A/CB partner violates any of these A/CB program Rules, the Corporation has the right to take action to correct and redress such violations including, without limitation, the imposition of assessments and/or the termination of the A/CB program on thirty (30) calendar days prior written notice.

The Corporation has the right to itself take such action, and to require the Customer, the A/CB partner, or both to take such action that the Corporation deems necessary or appropriate to determine and ensure on-going compliance with the Standards. Such action may include, but may not be limited to, mandatory transfer of the A/CB program to a third party and suspension or termination of the A/CB program.

The Customer associated with the A/CB partner indemnifies and holds the Corporation harmless from and against any claim arising from or related to an act or omission of the A/CB partner, including, without limitation, any claim arising from or related to the termination of the A/CB program.

5.2.6 Termination without Cause

The Corporation has the right to terminate any A/CB program, without cause, on at least ninety (90) calendar days prior written notice to the Customer and the A/CB partner. The Customer may appeal the termination by providing written notice to the Corporation within thirty (30) calendar days of receipt of the notice of termination. The appeal will be presented to the Board for review and decision. Any decision of the Board will be final.

5.3 A/CB Communication Standards

5.3.1 Standards for All Communications

All Solicitations, applications, advertisements, disclosures, and other material and information regarding any A/CB program (collectively for the purposes of this Rules chapter only, "Solicitations") must refer prominently to the offering as a "Maestro Card" and may not position the offering as something other than a Card. The A/CB brand name or logo may not be positioned as adding superior utility to the Card.

Any Solicitation regarding any A/CB program must prominently and integrally feature the Maestro word mark and Marks and must identify the Issuer.

A Solicitation may not imply or state that anyone other than the Customer is the Issuer of the Card.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and a regional Rule variation on this topic appears in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

5.3.2 Review of Solicitations

Each Solicitation must be submitted to and approved by the Corporation prior to final production and use.

A Solicitation that is a direct mail item (excluding electronic mail) or telemarketing operator script may be submitted to the Corporation for approval on an after-the-fact basis where timing is an unavoidable problem. In such event, the Solicitation must be received by the Corporation within two (2) business days after first being mailed or otherwise used. The Corporation must receive a sample of every final direct mail Solicitation.

5.4 A/CB Card Requirements

5.4.1 Card Design

All A/CB program Card designs must be reviewed and approved by the Corporation prior to final production and must comply with the Standards set forth in the MasterCard Card Design Standards.

5.4.2 Issuer Identification

The following Issuer identification requirements apply to all A/CB Cards:

1. neither the Card design nor any information appearing on the Card may state or infer that anyone other than the Customer is the Issuer of the Card;
2. Issuer identification consisting of the Issuer's name or the Issuer's name and logo must be clearly visible either on the Card face or on the Card back. The name and/or logo of an A/CB partner may appear on the Card face, in addition to the Issuer identification, or on the Card back;
3. Cards that bear only the A/CB partner's name or logo on the Card face, but that satisfy the Issuer identification requirements set forth in (5.) below, are deemed (in the absence of other circumstances) to comply with these requirements;
4. in addition to, or in lieu of, appearing on the upper portion of the Card face, the name of the A/CB partner may be embossed on the fourth line of embossing;
5. if the Issuer identification does not appear on the Card face, the following statement must prominently appear and be clearly legible on the Card back: "This card is issued by (FULL, TRUE ISSUER NAME) under license from MasterCard International or its Affiliates." The location of this statement on the Card is at the Issuer's discretion;
6. for A/CB programs in which more than one A/CB partner is involved, Issuer identification on the Card back must be equal or greater in size than any A/CB partner identification on the Card back;
7. the Issuer's customer service telephone number must appear on the back of all A/CB Cards. The location of the number is at the Issuer's discretion.

5.4.3 A/CB Card Design—Partner's Identification—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

5.4.4 A/CB Card Design—Program Names—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

5.5 A/CB 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 Marks

The Marks must be displayed on a stand-alone basis apart from any A/CB partner identification at any POI Terminal that accepts Cards.

The 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 Corporation has the right to require the modification of any POI Terminal display of an A/CB program name or logo that the Corporation determines does not comply with these Rules or adversely affects the Marks.

The A/CB program Card face design may not be used as an element of any Merchant decal.

5.6 Prepaid Card Programs

A Prepaid Card Program means:

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

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

5.6.1 Responsibility for the Prepaid Card Program

The Issuer is responsible for its Prepaid Card Programs, the Prepaid Card Program funds associated with those Prepaid Card Programs, and for the actions (or inaction) of any agents it uses in connection with such Prepaid Card Programs. The Corporation exclusively determines if an Issuer is in compliance with the foregoing requirements.

5.6.2 Categories of Prepaid Card Program

The Corporation categorizes Prepaid Card Programs into three categories: consumer, commercial, and government. The Corporation may adopt additional and/or review the current categories of Prepaid Card Programs from time to time in its sole discretion.

5.6.2.1 Consumer Prepaid Card Programs

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

5.6.2.2 Commercial Prepaid Card Programs

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

5.6.2.3 Government Prepaid Card Programs

Government Prepaid Card Programs are Prepaid Card Programs in which the funds are deposited in the prepaid Account by a government entity. Government Prepaid Card Programs are designed to deliver government payments to a person, including, but not limited to, segmented non-taxable wages, social benefits, pensions and emergency assistance, as governed by applicable law. In the case of Government Prepaid Card Programs, the funds deposited in the prepaid Account may be owned by the government entity or by the consumer or other third party designated by the government entity or such consumer. If the government entity permits a consumer to deposit funds in the prepaid Account owned by the government entity, the Government Prepaid Card Program becomes a Consumer Prepaid Card Program and all relevant Consumer Prepaid Card Program requirements apply.

5.6.3 Return of Unspent Value

Issuers must return any unspent funds in the prepaid Account to the owner of that Account in compliance with applicable law or regulation. In instances where applicable law or regulation does not provide time frames concerning the return of unspent funds, Issuers must comply with the requirements set forth in this Rule 5.6.3. Subject to applicable law or regulation, an Issuer has no obligation to return unspent funds in the prepaid Account if the identity of the owner of the unspent funds has not been provided to the Issuer.

5.6.3.1 Consumer Prepaid Card Programs

Issuers of Consumer Prepaid Card Programs must provide the consumer with a minimum of twelve months from the date of the last value load or thirty calendar days after the expiration date, whichever comes later, to request the return of unspent funds, less any applicable fees imposed by the Issuer or any other lawful offsets. Prominent disclosure must be made to the consumer as to how and when to request the refund of unspent funds and as to any fees that apply to the Prepaid Card Program. Once the consumer submits a refund request, the consumer must receive a refund of unspent funds within thirty calendar days of the date on which the refund request was received by the Issuer.

5.6.3.2 Commercial Prepaid Card Programs

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

5.6.3.3 Government Prepaid Card Programs

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

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

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

5.6.4 Value Loading

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

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

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

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

5.6.5 Communication and Marketing Materials

If an Issuer's prepaid Cards are intended to be used by Cardholders for personal, family or household use, then the Issuer must provide Cardholders with the terms and conditions of the Prepaid Card Program on or before any purchase is made or activation fees are incurred. If the Issuer's prepaid Cards are intended to be used by Cardholder for business use, then the Issuer must provide the commercial entity or government entity, as the case may be, with the terms and conditions of the Prepaid Card Program on or before any purchase is made or activation fees are incurred. Thereafter, the Issuer must provide the respective Cardholder, commercial entity or government entity with any amendment or modifications thereto and, in particular, make clear and conspicuous disclosures with respect to all fees to be incurred by the prepaid Account holder to obtain, use, reload, maintain and/or cash out the balance in the prepaid Account or for any other use, as required by the Standards and applicable law.

Issuers must submit all communications and marketing materials including, but not limited to, printed materials and copies or electronic versions of Web sites and mobile applications, if any, for all Prepaid Card Programs to the Corporation via e-mail at brand_standards@mastercard.com for review and approval prior to the launch or subsequent modification of the Prepaid Card Program and prior to any marketing of the Prepaid Card Program. The Corporation review is limited to compliance with the Standards for Issuer communications. Each Issuer is responsible for ensuring that its Prepaid Card Program communication and marketing materials comply with applicable law and the Standards. Communication and marketing materials include, but are not limited to, card carriers, press releases, Web sites, welcome letters, consumer applications, and terms and conditions.

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

Issuers of prepaid Cards intended to be used by Cardholders for personal, family or household use must inform Cardholders if their prepaid Cards are linked to a selective authorization Program. Issuers of prepaid Cards intended to be used by Cardholders for business use must inform the commercial entity or government entity, as the case may be, of the foregoing. Refer to the *Selective Authorization Communications Policy* available on MasterCard Connect for additional information.

5.6.6 Anti-Money Laundering

Issuers of Prepaid Card Programs must do so in compliance with the MasterCard Anti-Money Laundering Program (the "AML Program"). The AML Program requires Issuers to have an anti-money laundering compliance program that, at a minimum, includes policies, procedures, and controls for customer identification and ongoing due diligence, appropriate limitations on anonymous activities, suspicious activity monitoring and reporting, record-keeping procedures, independent controls testing and sanction screening. Issuers must screen their Cardholders pursuant to the economic and trade sanctions requirements of the Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury.

The Corporation may perform periodic reviews of the Issuer's anti-money laundering compliance program to ensure ongoing compliance with the AML Program. As part of this periodic review, Issuers may be subject to enhanced due diligence procedures which may include on-site examinations and/or the use of a third party reviewer.

Any violation of the AML Program and requirements could lead to noncompliance assessments, immediate Prepaid Card Program or suspension and/or termination of License.

5.6.7 Anonymous Prepaid Card Guidelines

Refer to the *Guidelines for Anonymous Prepaid Card Programs* available on MasterCard Connect for additional information regarding anonymous prepaid card policies.

5.6.8 BINs

Issuers must use a dedicated BIN(s) and associated prepaid product codes in conjunction with their Prepaid Card Programs.

5.7 Chip-only Card Programs—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
5.2 Affinity and Co-Brand (A/CB) Card Programs	A
5.3 A/CB Communication Standards	B
5.4 A/CB Card Requirements	B
5.5 A/CB Acceptance RequirementsRequirements	A
5.6 Prepaid Card Programs	A

Chapter 6 Issuing

This chapter contains information about issuing requirements.

6.1 Eligibility

6.1.1 Eligible Cards

The Corporation determines the requirements regarding which cards issued by its Customers may bear the Marks, except that:

1. the Customer must actually maintain the deposited funds on Account; and
2. the Customer must not place the Marks on any card that has access to any of the following types of accounts:

   a. charge card or credit card account as the primary account;

   b. accounts that "pass-through" to an account at an institution not qualified to join as a Customer;

   c. accounts linked to cards issued under special issuer programs except where such programs have received written approval from the Corporation. (See Chapter 5, "Special Issuer Programs," of this rulebook and applicable regional Rules for further information about affinity and co-branded cards).

All Cards must conform to the requirements of the MasterCard Card Design Standards System available on MasterCard Connect.

NOTE

A regional Rules variation on this topic appears in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

6.1.1.1 Eligible Mobile Payment Devices

The Rules set forth in Rule 6.1.1 above apply to a Mobile Payment Device, except there is no limitation on the types of account that may co-reside on the same Mobile Payment Device user interface, so long as such accounts are not linked, but rather exist independently and are accessed by a separate and distinct payment application hosted on the same user interface.

6.1.2 Gateway Processed ATM Transactions

If a card which is an access device for a competing network or a card which the Corporation has approved for processing to another network which does not participate in the Corporation ("Gateway Processing") is used in a Terminal and the resulting transaction is routed through the Interchange System, the Principal which sends the transaction to the Interchange System will be deemed to have consented to all applicable Rules of the Corporation and to have agreed to pay all Corporation fees in connection with such transaction.

6.1.3 Eligible Accounts

Customers may make only the following types of accounts available for access, directly or indirectly, through the Interchange System:

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

Each Issuer must provide its Cardholders, wherever domiciled, with access to their Cardholders' Accounts in the country where such Issuer is Licensed, and in such additional countries as permitted by the Corporation.

NOTE

Regional Rule variations on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.1.3.1 Ineligible Accounts

Any account held or serviced by an Acquiring-only Customer is not eligible to be an Account. This provision does not prevent a Customer from using the Interchange System to route ATM transactions to a network which does not participate in the Corporation, if such use has been authorized by the Corporation and is expressly permitted in the Rules.

6.1.4 Program Names

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.2 Card Standards and Specifications

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

NOTE

Refer to Appendix B, "Technical Specifications," for additional information about standards referred to in this section.

Any Issuer that allows a Cardbase to access the Interchange System must comply with Rule 6.2, except in the case of a Mobile Payment Device. An Issuer of a Mobile Payment Device must comply with Rules 6.2.1.3, 6.2.1.4, and 6.2.1.8.

Any Issuer that allows any new Cardbase access to the Interchange System must use a prefix number, as defined in Rule 6.2.1.3 of the Rules. New Cardbases that do not fully comply with Rule 6.2.1.3 must be replaced by fully compliant Cards within nine (9) months of the date on which such Cardbase first had access to the Interchange System.

The physical characteristics of Cards must be consistent with both:

1. ISO 7810 Identification cards—physical characteristics; and
2. ISO 7813 Identification cards—financial transaction cards.

6.2.1 Encoding Standards

Each Card must have a magnetic stripe. It is strongly recommended that Issuers use a high coercivity magnetic stripe that is consistent with ISO 7811/6.

The magnetic stripe characteristics must be consistent with:

1. ISO 7811/2 LoCo Magnetic stripes;
2. ISO 7811/4 Location of Magnetic track 1 and 2;
3. ISO 7811/5 Location of Magnetic track 3;
4. ISO 7812/1 and 7812/2 Identification cards—Numbering system and registration procedure for issuer identifiers.

6.2.1.1 Track 1

Issuers are strongly recommended to encode track 1. If track 1 is encoded, it must comply with the Rules and ISO 7813.

Issuers are advised that the encoding of track 1 may be required by the Corporation, for other uses in the industry (POS), at some future date.

Track 1 must not be used for authorization purposes.

6.2.1.2 Track 2 Format

Issuers must encode track 2 data in full compliance with ISO 7813, and the encoding specifications as detailed in Appendix B, "Technical Specifications."

The following minimum data must be encoded on track 2 of a Card:

1. start sentinel
2. primary account number
3. field separator
4. expiration date
5. service code

6. end sentinel
7. longitudinal redundancy check

The maximum total digits that may be encoded on track 2 is forty (40).

6.2.1.3 Primary Account Number (PAN)

The PAN must be no less than twelve (12) and no more than nineteen (19) digits in length. All digits of the PAN must be numeric.

Transactions must be capable of being routed for authorization based on the first two (2) to eleven (11) digits of the PAN.

Effective 1 January 2007, the PAN that appears on the face of the Card must be the same as the PAN encoded in the magnetic stripe and chip, if present. This requirement does not apply in the case of a Mobile Payment Device.

The following three (3) sub-fields comprise the PAN:

1. Issuer Identification Number (IIN) or Bank Identification Number (BIN):

   Cards of existing Customers may have a routing prefix of between four (4) and eleven (11) digits in length, which must conform to ISO 7812/1 approved values.

   A Cardbase must use a prefix number that is recognized by ISO.

   The IIN appears in the first six (6) digits of the PAN and must be assigned by the ISO Registration Authority, or a delegated authority such as MasterCard, and must be unique. This prefix will start with 50XXXX, 560000 through 589999, or 6XXXXX, but not 59XXXX. Cards that bear both the MasterCard brand and the Marks will use a MasterCard assigned IIN in the range of 510000 through 559999.

   It is strongly recommended that all Customers, but particularly such Customers who became Customers of the Corporation after January 2001, issue Cards with the routing information limited to six (6) digits.

   POS Acquirers will only be required to route on the first six (6) digits of the prefix within the routing table. In the future, POS and ATM exception processing will use six (6)-digit routing to identify the Customer.

2. Individual Account Number:

   The individual account number must not be the same as the complete routing/sorting and the actual bank account numbers.

3. Transposition Check Digit:

   The individual account number must be followed by an ISO 7812/1 Transposition Check Digit, which is calculated on all digits of the PAN, including the Issuer Identification Number (IIN). The Transposition Check Digit must be computed according to the Luhn formula for modulus 10 check digit as described in Appendix B, “Technical Specifications.”

If the Corporation notifies a Principal that a prefix number it sponsors is invalid, the Issuer must replace all its Cards that use such prefix number within three (3) months from date of notice. A prefix number is considered invalid when the Issuer cannot produce written authorization of prefix assignment from ISO or its designated representative(s). On the first Interchange System Business Day following the three (3) months date of notice, the prefix number sponsored by such Principal will be reassigned appropriately in the Interchange System routing tables.

If it is discovered that more than one (1) entity validly owns a prefix number, as evidenced by written authorization from ISO or its designated representative(s), the entity that receives final assignment from ISO is determined to be the rightful owner of such prefix number insofar as participation in Transaction interchange in the Corporation is concerned.

If the Corporation notifies any Principal that a prefix number it sponsors is in conflict with a prefix number of an entity that wishes to participate in Transaction interchange in the Corporation, and such entity has established prior rightful ownership of such prefix number, the Issuer currently using such prefix number must replace all Cards that use such prefix number within three (3) months from date of final assignment by ISO and certify compliance to the Corporation. On the first Interchange System Business Day three (3) months after ISO makes its final assignment, the prefix number sponsored by such Principal will be reassigned appropriately in the Interchange System routing tables.

6.2.1.4 Expiration Date

The expiration date must be a valid future date, four (4) digits in length, and structured in a year-month format (YYMM).

Cards must not use a maximum validity period of more than twenty (20) years from the date of issuance or, for non-expiring Cards, the designated default value of 4912 (December 2049) must be used.

The expiration date of a hybrid Card must not exceed the expiration date of any of the certificates contained within the chip on the hybrid Card. In the case of a non-expiring hybrid Card, the following conditions must be met:

1. The settings within the chip contained on the hybrid Card must force every Transaction online for authorization or decline the Transaction if online authorization is not possible;
2. The hybrid Card must not contain an offline CAM certificate; and
3. The Issuer must utilize full EMV processing.

For additional information, refer to the chip technical specifications.

6.2.1.5 Service Code

The service code must be numeric, and must comply with ISO 7813.

It is strongly recommended that Issuers encode extended service code values 120 (or 220)—online authorization, PIN required—on Cards for which Maestro is the primary acceptance brand. Note: This does not apply to Maestro-branded MasterCard cards, as the primary acceptance brand in this instance is MasterCard.

The only acceptable values for encoding new or re-issued Cards are as follows:

Position	Value	Description
1	1	Available for International Interchange
	2	Available for International Interchange(alternative technology—Chip Card)
2	0	Normal authorization
	2	Positive online authorization required
3	0	PIN required
	1	Normal Cardholder verification, no restrictions
	6	Prompt for PIN if PIN pad present

Issuers that encode value "0" (normal authorization) in position 2 of the extended service code must accept liability for any purchase Transaction completed at a cardholder-activated terminal (CAT).

Issuers that encode values "1" (normal Cardholder verification, no restrictions) or "6" (prompt for PIN if PIN entry device present) in position 3 of the extended service code must not decline Transactions simply because they do not contain a PIN.

Effective 1 January 2007, all Cards must use the values contained in the chart above for encoding purposes. No other values will be allowed.

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

6.2.1.6 Discretionary Data

All other encoded data not listed in Rule 6.2.1.2 is discretionary data, and under the Issuer's control.

This data is routed to Issuers for manipulation and verification in messages, as specified in the applicable technical specifications.

This data must be encoded between the service code and the end sentinel, and only contain valid characters in accordance with ISO 7813.

It is recommended that the discretionary data field be encoded as specified in Appendix B, "Technical Specifications."

Issuers, at their option, may encode CVC 1 on track 1 and track 2 in three contiguous positions in the discretionary data field of the magnetic stripe of a Card. For additional information about CVC 1 calculation methods and encoding standards, refer to Appendix B, "Technical Specifications."

6.2.1.7 Card Application Software and Personalization of Chip Cards

The card application software of Chip Cards must comply with the chip technical specifications, as published from time to time, by the Corporation.

The personalization data of Chip Cards must comply with Card issuance requirements set forth in the chip technical specifications, as published from time-to-time by the Corporation.

In addition, the chip application of hybrid Cards must be type-approved by the Corporation before Card issuance.

6.2.1.8 Application Software and Personalization of Maestro on Access Devices and Mobile Payment Devices

The application software and personalization data for a Maestro *PayPass* Access Device or Mobile Payment Device must comply with the technical specifications, as published from time to time by the Corporation.

NOTE

An additional regional Rule on this topic appear in Chapter 20, "United States Region," of this rulebook.

6.2.1.9 Encoding of PIN Verification Value (PVV)

Issuers are strongly encouraged to encode a PIN Verification Value (PVV) and to use the formula defined by the Corporation as shown in the technical specifications. If a proprietary algorithm is used for the calculation of a PVV, or the PVV is not encoded, Transactions authorized using the Stand-In Processing Service will be authorized without PIN validation.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.2.1.10 Track 3

Track 3 may be encoded, but it is not used for Transaction processing.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.2.2 Embossing and Engraving Standards

1. Cards must be embossed, laser engraved, indent printed, or hot stamped, in full compliance with ISO 7811 and with the Identity Standards.
2. The Issuer name must be printed on the Card.
3. An Issuer's, or its Corporation-approved agent's, customer service phone number must be printed on the Card back.
4. The Cardholder's name may be either embossed, laser engraved, indent printed, or hot stamped on the front of the Card. It is strongly recommended that the Issuer include the Cardholder's name on magnetic-stripe only Cards.
5. The Primary Account Number (PAN) must be embossed, laser engraved, indent printed, or hot stamped on the front of all Cards issued on or after 1 January 2007. Effective 1 January 2010, the PAN must be embossed, laser engraved, indent printed, or hot stamped on the front of all Cards.
6. The expiration date may be embossed, laser engraved, indent printed, or hot stamped on the front of the Card.
7. Any additional data may be included at the discretion of the Issuer, but may not take precedence over the minimum identification requirements set forth in the Rules.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.2.3 Chip Card Standards

Chip Cards must support magnetic stripe technology.

To protect against the risk of counterfeiting, the track data on the magnetic stripe of the Card must not be reproducible from the Track 2 Equivalent Data on the chip. This means that some aspect of the magnetic stripe track data must be unique to the magnetic stripe and unpredictable. Using all or part of a PAN/Card Sequence Number or all or part of the "Valid From" or expiration date does not qualify as "unpredictable."

Effective 11 January 2013, newly issued or re-issued Cards that carry a PAN of 16 digits or less must support a CVC 1 on the magnetic stripe and a Chip CVC in the Track 2 Equivalent Data. Chip grade Issuers must use a different value for Chip CVC than the CVC 1 encoded on the magnetic stripe.

The Maestro payment application must conform to the chip technical specifications as published from time to time by the Corporation.

All Chip Cards must have a single primary application that resides on the chip and on the magnetic stripe; the PAN, when appearing on the Card front in accordance with Rule 6.2.2(e), must be for the primary application resident on the magnetic stripe.

The Issuer of a Chip Card must implement M/Chip as the EMV payment application on the Card, in accordance with a current M/Chip Card application specification.

Chip Cards may support any stored value or non-payment application provided it is approved in writing by the Corporation.

The service marks of stored value and non-payment applications must be used in accordance with the Identity Standards.

Prior to placement and use of an application on a Chip Card, an Issuer, or any party acting at the Issuer's request, must notify the Corporation or its agent.

The Corporation or its agent reserves the right, on an exceptional basis, to disapprove the application. All such applications must conform to all applicable technical specifications as published from time to time by the Corporation.

Any operating system(s) to be placed on a Chip Card by any Issuer or by any other party at an Issuer's request must meet Corporation defined security requirements before use.

Prior to Chip Card production and distribution, Issuers must receive a Compliance Assessment and Security Testing (CAST) certificate number from their vendors. For information regarding CAST refer to the *Compliance Assessment and Security Testing Program* manual or contact the Chip Help Desk at chip_help@mastercard.com.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and in Chapter 20, "United States Region," of this rulebook.

6.2.3.1 Chip Card Validation Code (CVC)

If an Issuer chooses to encode CVC 1 on the magnetic stripe of its Cards, the Issuer must encode Chip CVC in the track 2 equivalent data in three contiguous positions of the discretionary data field of the chip on all Chip Cards.

Full grade chip Issuers and Magnetic Stripe Grade Issuers (that have the capability to distinguish between chip-read and magnetic stripe-read Transactions) must use a different value for CVC 1 than for the Chip CVC for all Chip Cards issued on or after 1 January 2008.

If a Magnetic Stripe Grade Issuer cannot distinguish between chip-read and magnetic stripe-read Transactions, the Issuer may use the same value for CVC 1 and Chip CVC. All Magnetic Stripe Grade Issuers must use a different value for CVC 1 than for a Chip CVC for all Chip Cards issued on or after 18 October 2013. For Magnetic Stripe Grade Issuers in Brazil, this requirement takes effect on 12 October 2012.

For CVC calculation methods and encoding standards, refer to Appendix B, "Technical Specifications."

Refer to the chip technical specifications additional information.

6.2.3.2 Maestro *PayPass* Contactless Payment Functionality

Issuers may add the Maestro *PayPass* contactless payment functionality to their Chip Cards. If an Issuer chooses to add this functionality to its Chip Cards, it must comply with the requirements set forth in this Rule 6.2.3, the Maestro *PayPass* technical specifications, and the Identity Standards, as may be in effect from time to time.

6.2.3.3 Card Authentication

Chip Cards must support dynamic online CAM. In addition, Chip Cards that perform Transactions offline must support offline CAM. Although both static and dynamic offline CAM are permitted, it is strongly recommended that Chip Cards support dynamic offline CAM.

All Maestro *PayPass* Cards must support Combined Data Authentication (CDA) and must not support other forms of offline CAM on the contactless interface. For additional information, refer to the Maestro *PayPass* technical specifications.

NOTE

A regional Rule variation on this topic appears in Chapter 20, "United States Region," of this rulebook.

6.2.3.4 Chip Card and Chip Transaction Plans—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.2.4 Mobile Payment Device Standards

A Mobile Payment Device may support Maestro *PayPass* functionality. If an Issuer chooses to add this functionality to its Mobile Payment Device, the application software, personalization data, and all other aspects of the functionality must comply with the requirements set forth in the Standards, including but not limited to, the applicable technical specifications, and the Identity Standards, as may be in effect from time to time. Issuers should also refer to the mobile payment security guidelines set forth in *Security Guidelines for Mobile Payment Solutions*.

The *PayPass* application must be implemented within a secure IC (the Secure Element [SE]). The SE must be CAST-approved and have received a mobile payment certificate number (MPCN). All CAST-approved SEs (with corresponding MPCN) from which Issuers can choose from are listed on MasterCard Connect—the Mobile Payment Device itself does not undergo a CAST approval. The *PayPass* application must also pass the functional and security testing program, for which a letter of approval will be issued by the Corporation.

6.2.5 Signature Panel

NOTE

A regional Rule variation on this topic appears in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

Each Card must contain either:

1. a signature panel on the Card; or
2. a signature that is laser engraved.

The placement and size of the signature panel must be in full compliance with the Identity Standards.

6.2.5.1 Approved Signature Representation Method(s)—Europe Region Only

NOTE

A regional Rule on this topic appears in Chapter 17, "Europe Region," of this rulebook.

6.2.6 Adhesive Material on Cards

Customers must not put adhesive material on a Card that may interfere with the recognition of the Marks or the normal operation of any POI Terminal or Card.

Other than any adhesive materials used to affix the chip to the Card during the manufacturing process, no adhesive materials of any kind may be applied on the magnetic stripe or within the chip safety area, (as defined in the MasterCard Card Design Standards System available on MasterCard Connect).

The Marks must not be displayed on Cards by use of adhesive stickers.

6.3 Optional Card Security Features

Issuers are recommended to use the following optional Card security features:

1. the Maestro hologram;
2. the Maestro tamper evident signature panel;

3. a Cardholder photograph; and/or
4. the Maestro UV mark.

If an Issuer chooses to use one or more of the optional Card security features referenced above, the Issuer must comply with the guidelines for those features set forth in the MasterCard Card Design Standards System.

NOTE

Regional Rule variations on this topic appear in Chapter 17, "Europe Region," and in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

6.4 PIN and Signature Requirements

Cardholders must be verified by a PIN, whether magnetic stripe or chip is used to initiate the Transaction, except in the case of properly presented Maestro *PayPass* Transaction where no CVM is required and parking garage and tollway Transaction conducted in the Europe Region as set forth in Rules 9.4.4 and 9.4.5 of Chapter 17 of this rulebook.

Additional regional Rules and Rule variations on this topic appear in Chapter 17, "Europe Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

6.4.1 PIN Issuance

Issuers must issue PINs to all Cardholders.

The PIN must be at least four (4) and no more than six (6) characters in length.

ISO allows for up to twelve (12) character PINs, but for the purpose of receiving incoming Transactions, Issuers must be capable of verifying PINs based on a maximum of six (6) characters, as interregional processing only supports numeric PINs from four (4) to six (6) digits in length.

Issuers should advise their Cardholders that many PIN entry devices only contain numeric values as alpha mapping is not required in some global locations. Issuers must provide their Cardholders with the numeric equivalent of the first six (6) alpha characters of the Cardholder's PIN as this information is required in some global locations.

NOTE

A regional Rule variation on this topic appears Chapter 16, "Canada Region," and Chapter 20, "United States Region," of this rulebook

6.4.2 Use of the PIN

All Cards must support online PIN verification as the CVM.

Issuers must verify their Cardholders by means of online PIN verification as the CVM if a magnetic stripe is used to initiate the Transaction except under the circumstances outlined in Rule 6.4.3 Use of PIN or Signature.

In addition, Issuer must verify their Cardholders by means of online PIN verification as the CVM for Mobile Remote Payment Transactions.

6.4.2.1 Chip Cards

In addition to the Rules set forth in Rule 6.4.2 above, the following applies:

1. Chip Cards must support both online PIN verification and offline PIN verification as the CVM for POS Transactions.

   NOTE

   A regional Rule variation on this topic appears in Chapter 20, "United States Region" of this rulebook.

   NOTE

   Issuers must define their priority of PIN verification methods within the chip.

   Offline PIN verification is recommended as the first priority. Refer to Rule 6.4.3 for additional information.

2. Chip Cards must support online PIN verification for ATM Transactions and PIN-Based In-Branch Terminal Transactions.
3. Issuers must comply with the detailed CVM requirements in the chip technical specifications as published from time to time by the Corporation.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

6.4.3 Use of PIN or Signature

Except for Maestro *PayPass* Transactions, Cardholders must be verified by a PIN, whether magnetic stripe or chip is used to initiate the Transaction, unless the Transaction is a POS Transaction that occurs at a hybrid POS Terminal in a country in which its Customers have received a waiver from the Corporation permitting hybrid POS Terminals to support offline PIN as the minimum CVM for a chip Transaction and signature as the CVM for a magnetic stripe Transaction. Such a waiver may be granted pursuant to the Corporation's approval of that country's Customers' plan(s) to implement EMV chip technology.

Those countries are:

1. Andorra
2. Belgium
3. Estonia

4. Finland
5. France
6. Iceland
7. Ireland
8. Latvia
9. Monaco
10. Portugal
11. Spain
12. United Kingdom

Issuers must accept and properly process (i.e., perform an individual risk assessment on each Transaction) any Transaction verified using a signature-based CVM in the same manner as it would if the Transaction had been verified using a PIN-based CVM.

Issuers will be indemnified for actual fraud losses suffered from Transactions verified by signature via the Issuer Assurance Plan, providing all requirements are met. Refer to Chapter 13, "Liabilities and Indemnification," for further information.

NOTE

Additional regional Rules and Rules variations on this topic appear in Chapter 15, "Asia/Pacific Region," Chapter 17, "Europe Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook.

6.5 Transmitting, Processing, and Authorizing Transactions

In order to authorize Transactions, an Issuer must maintain a direct functional 24-hour-per-day operating connection to the Interchange System or must ensure that any TPP(s) operating on its behalf maintains such a connection.

6.6 Fees to Cardholders

The Corporation does not determine whether any fee is charged to any Cardholders, or the amount of any such fee so charged. Issuers independently determine what fees, if any, to charge their Cardholders.

6.7 Stand-In Processing Service

An Issuer, at its option, may elect to support the Stand-In Processing Service for all POS and ATM Transactions.

An Issuer must support the Stand-In Processing Service if the Issuer became a Customer on or after 1 December 2003.

Regardless of when an Issuer became a Customer, an Issuer must support and implement the Stand-In Processing Service if:

1. the Issuer received notification from the Corporation that it has a substandard level 2 Issuer failure rate (refer to Chapter 9 of the Rules for additional information); or
2. the Corporation mandates the use of the Stand-In Processing Service.

NOTE

Additional regional Rules and a Rule variation on this topic appear in Chapter 20, "United States Region," of this rulebook.

6.7.1 Minimum Transaction Limits

The Corporation will set a minimum daily Stand-In Processing Service Transaction limit per Card. An Issuer may, at its option, increase the daily Stand-In Processing Service Transaction limits set by the Corporation. The Corporation may set a lower minimum Stand-In Processing Service Transaction limit for prepaid Cards that are issued under a BIN that is different than the BIN used for its Cards other than its prepaid Cards.

If use of the Stand-In Processing Service is mandated by the Corporation, the Corporation may select an alternative minimum daily Stand-In Processing Service Transaction limit to be applied to POS and ATM Transactions.

6.7.1.1 Minimum Transaction Limit for POS Transactions

The minimum daily Transaction processing limit for POS Transactions is:

1. USD 250 (or its local currency equivalent); or
2. three Transactions for the purchase of goods and services (other than a Merchandise Transaction conducted at an ATM);
3. whichever occurs first.

6.7.1.2 Minimum Transaction Limit for ATM Transactions

The minimum daily Transaction processing limit for ATM Transactions is:

1. USD 125 (or its local currency equivalent); or
2. two ATM Transactions;
3. whichever occurs first.

6.7.2 PIN Validation

Issuers are strongly recommended to establish Stand-In Processing Service PIN validation with the Corporation.

Issuers that are mandated to use the Stand-In Processing Service have one (1) month before the commencement of Stand-In Processing Services to establish PIN validation with the Corporation. Failure to establish PIN validation services with the Corporation within the prescribed time frame will result in the implementation of Stand-In Processing Service without PIN validation.

Issuers may request that the Corporation forgo Stand-In Processing Service PIN validation.

For additional information, refer to the applicable technical specifications manual.

6.8 Mobile Remote Payment Transactions

The Standards in this Rule 6.8 apply in countries where Mobile Remote Payment Transactions are supported. The applicability of these Standards in a country will be announced in a regional and/or country-specific bulletin.

6.8.1 Issuer Domain Mobile Remote Payment Transactions

Issuers that permit their Cardholders to perform Mobile Remote Payment Transactions must register with the Corporation. Refer to the *Mobile Remote Payments Program Guide* for additional information.

An Issuer may use a Service Manager to provide Mobile Remote Payment Program Service. Issuers using a Service Manager to participate in a Mobile Remote Payment Program must ensure the Service Manager complies with all applicable Standards, including the branding requirements and the security requirements and guidelines for Mobile Remote Payment. Refer to the *Mobile Remote Payments Program Guide* for additional information.

The Issuer must register each Service Manager proposed to provide Mobile Remote Payment Program Service as a Third Party Processor, as set forth in Rule 14.6 of this rulebook.

A Mobile Remote Payment Transaction must not be effected using Maestro *PayPass* contactless payment functionality.

6.8.2 Issuer Responsibilities

Issuers that offer Issuer Domain Mobile Remote Payment Transaction programs must:

1. Provide Cardholders that want to participate in Issuer Domain Mobile Remote Payment Transactions with a PAN between thirteen (13) to nineteen

(19) digits in length. The PAN must start with a BIN. (The BIN can be the one that is currently used by the Issuer). The Issuer may optionally use a pseudo PAN, (a PAN that is different from the PAN displayed on the Cardholder's physical card). If a pseudo PAN is used, it must be static;

2. Complete the expiration date field. This four (4)-digit field may be used for the actual expiration date of the Card, which must not exceed five (5) years. The format of the field is as follows:

   a. the first two (2) digits must be a value between 01 and 12; and

   b. value of the next two (2) digits must not be equivalent to more than five (5) years after the Transaction year;

3. Comply with the branding requirements in the *Mobile Remote Payments Program Guide*,

4. Ensure that its authorization system provides a valid response code as identified in the authorization message. "Call Me" is not a permitted response. Mobile Remote Payment Transactions may be approved or declined only; and

5. Implement security techniques between the Cardholder Mobile Device for Personal PIN Entry and the Issuer server to guard against unauthorized Transactions. In addition, Issuers must provide implementation, registration, and instructions for Cardholders or delegate a specific implementation and registration function to a Service Provider. Refer to the *Mobile Remote Payments Program Guide* for additional information.

Issuers may choose to implement mobile specific credentials and a method of generating an Accountholder Authentication Value (AAV), as an alternative to using PIN as the CVM for Issuer Domain Mobile Remote Payment Transactions. If an Issuer chooses to implement this method, it must provide clear communication to the Cardholder regarding the process to conduct an Issuer Domain Mobile Remote Payment Transaction without the use of PIN as the CVM. Refer to the *Mobile Remote Payments Program Guide* for additional information.

6.8.3 Issuer Responsibilities: Acquirer Domain Mobile Remote Payment Transactions

Issuers must recognize properly identified Acquirer Domain Mobile Remote Payment Transactions. If an Acquirer Domain Mobile Remote Payment Transaction is reported as a fraudulent Transaction, and the Remote Payments Program Type has a value of 2 (Acquirer Domain) was present in Data Element 48, subelement 48, subfield 1 (Mobile Program Indicators), Issuers will have a chargeback right.

6.9 Electronic Commerce

Issuers must recognize properly identified electronic commerce Transactions and, if authorized, take responsibility for fraud, unless it can be proved that the Merchant and/or Acquirer participated in the fraud. However, if the authorized Transaction contained the Corporation-assigned static AAV in the UCAF field, Issuers will have a chargeback right for fraudulent Transactions.

Issuers are not mandated to allow their Cardholders to perform electronic commerce Transactions, but they are recommended to do so.

An electronic commerce Transaction must not be effected using Maestro *PayPass* contactless payment functionality.

Stand-In processing services must not be used for electronic commerce Transactions.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and Chapter 19, "South Asia/Middle East/Africa Region," of this rulebook.

6.9.1 Issuer Responsibilities

Issuers that support electronic commerce Transactions and use *SecureCode* to verify their Cardholders must provide and keep updated information for display on the Web site listed below. Refer to the *MasterCard SecureCode—Issuer Implementation Guide* for further information.

mastercard.com/securecode

1. In addition, Issuers that support electronic commerce Transactions must:

   a. provide Cardholders wishing to participate in electronic commerce Transactions with an account number PAN of between thirteen (13) to nineteen (19) digits in length. The PAN must start with a Maestro BIN. (The BIN can be the one that is currently used by the Issuer). The Issuer may optionally use a pseudo PAN, (a PAN that is different from the PAN displayed on the Cardholder's physical card). If a pseudo PAN is used, it must be static;

   b. complete the expiration date field. This four (4)-digit field may be used for the actual expiration date of the Card, which must not exceed five (5) years. The format of the field is as follows:

      - the first two (2) digits must be a value between 01 and 12; and
      - the value of the next two (2) digits must not be equivalent to more than five (5) years after the Transaction year.

   c. ensure that its authorization system provides a valid response code as identified in the authorization message. "Call Me" is not a permitted

response. Electronic commerce Transactions may be approved or declined only;

d. process (that is, perform risk assessment) any Transaction for which the UCAF field (data element 48, sub-element 43) contains the Corporation-assigned static AAV;

e. implement security techniques between the Cardholder interface device and the issuer server to guard against unauthorized Transactions.

2. Issuers should:

a. provide a registration and set up process for Cardholders wishing to perform electronic commerce Transactions;

b. ensure that Cardholder authentication information is properly registered;

c. properly identify Cardholders if issuing certificates;

d. educate Cardholders of the risks of releasing Card details and PINs into open networks and entering PINs into public terminals without using the approved methods.

3. Issuers may choose:

a. to implement MasterCard *SecureCode* directly and register Cardholders or delegate a specific implementation and registration function to a designated service provider (according to the set-up requirements provided to the Corporation by the Issuer);

b. to request the Cardholder to use a chip/hardware authentication device;

c. the Cardholder verification method (if any) which is to be used.

6.9.2 MasterCard Advance Registration Program (MARP) Transactions

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.10 Selective Authorization

Without the express prior written approval of the Corporation, a Customer may not launch or maintain a Card Program for the purpose of selectively authorizing Transactions arising from use of Program Cards at only a subset of Maestro acceptance locations. A Customer is not prohibited from authorizing or declining individual Transactions based on:

1. the amount of funds or overdraft credit available;
2. fraud risks presented by individual Cardholder usage patterns;
3. cash access restrictions to manage a high risk Account;

4. Cardholder-designated restrictions on use; or
5. Any other restriction on use the Corporation may permit.

NOTE

Additional regional Rules on this topic appears in Chapter 16, "Canada Region," Chapter 17, "Europe Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook.

6.11 MasterCard *MoneySend* Payment Transaction

A MasterCard® *MoneySend*™ Payment Transaction is a transfer of funds to an Account via the MasterCard *MoneySend* platform through the Interchange System.

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.11.1 MasterCard *MoneySend* Payment Transaction Requirements

Only Issuers that are approved and registered by the Corporation to receive MasterCard *MoneySend* Payment Transactions may do so.

Issuers must make either the PAN or a pseudo PAN available to all Cardholders. If the Issuer provides the Cardholder with a pseudo PAN, the Issuer must be able to identify the pseudo PAN with the Cardholder's actual PAN.

A participating Issuer must not decline a MasterCard *MoneySend* Payment Transaction based solely on the Transaction type and/or the Acquirer originating the Transaction.

The Issuer must identify each MasterCard *MoneySend* Payment Transaction on the Cardholder's periodic billing statement, including the amount of the MasterCard *MoneySend* Payment Transaction, the date of posting to the Account and the name of the sender.

The Issuer receiving a MasterCard *MoneySend* Payment Transaction authorization request may:

1. approve or reject any requests by the Acquirer to correct a clerical error; and/or
2. establish its own maximum MasterCard *MoneySend* Payment Transaction amount.

The Issuer must make the transferred funds available to the recipient without unnecessary delay. If funds will not be available immediately upon approval of the financial authorization request, the Issuer must inform the recipient when the funds will become available.

A MasterCard *MoneySend* Payment Transaction (MCC 6536 or 6537) must be effected in a way that does not conflict with Cardholder agreements or instructions.

NOTE

Regional Rules and a regional rule variation on this topic appears in Chapter 17, "Europe Region" of this rulebook.

6.12 Payment Transaction

Issuers that offer the Payment Transaction must make either the PAN or a pseudo PAN available to all Cardholders. If the Issuer provides the Cardholder with a pseudo PAN, the Issuer must be able to identify the pseudo PAN with the Cardholder's actual PAN.

It is strongly recommended that Issuers identify the Payment Service Provider on the Cardholder's statement.

The Issuer, at its discretion may:

1. authorize the Payment Transaction;
2. approve (and receive remuneration for costs incurred) or reject any requests by the Acquirer to correct a clerical error;
3. establish a maximum Transaction amount; or
4. determine when to make the transferred funds available to the recipient—immediately or after a period of time defined by the Issuer.

A Payment Transaction (MCC 6532 or 6533) must be effected in a way that does not conflict with Cardholder agreements or instructions.

6.13 Issuer Responsibilities to Cardholders

Each Issuer must fully comply with all applicable laws, Rules and regulations, including but not limited to those requiring initial disclosure and periodic reporting statements to Cardholders.

With respect to foreign currency, the Corporation highly recommends that the Cardholder statement show the original Transaction currency and amount, in addition to the amount billed in the Cardholder's currency, if different.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia Pacific Region," Chapter 16, "Canada Region," Chapter 17, "Europe Region," Chapter 19, "South Asia/Middle East/Africa Region," and Chapter 20, "United States Region," of this rulebook.

6.13.1 Limitation of Liability of Cardholders for Unauthorized Use

A Regional Rule on this topic appears in Chapter 17, "Europe Region Rules."

6.14 Fraud Reporting

"Fraud" is defined as being the reportable occurrence of a fraudulent Transaction performed using a Card regardless whether there was successful complete or partial recovery of the funds represented by such Transaction.

6.14.1 Reporting

An Issuer must use the System to Avoid Fraud Effectively (SAFE) to report monthly to the Corporation all fraudulent Transactions on Cards. For SAFE reporting procedures, refer to the *SAFE Products User Guide*.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.14.2 Completeness

An Issuer must report all fraudulent Transactions individually and all fraud types experienced by providing a fraud type code in the SAFE record for each fraudulent Transaction. For a listing and descriptions of fraud type codes, refer to Appendix A of the *SAFE Products User Guide*.

An Issuer with no reportable occurrences of fraudulent Transactions within the reporting month must submit a negative report.

6.14.3 Timeliness per Calendar Quarter

Fraudulent Transactions must be reported at least once per month. Eighty percent (80%) of all fraudulent Transactions must be reported to SAFE within sixty (60) days from the date of the Transaction or thirty (30) days from the Cardholder notification date. An Issuer that fails to meet the eighty percent (80%) performance standard will be subject to noncompliance assessments as set out below.

6.14.4 Penalties for Noncompliance

Occurrence	Penalty
First occurrence	Issuers' Primary Operations and Security Contacts receive notification by registered letter.
Second occurrence	Issuers' Primary Operations Contact receives notification by registered letter and is assessed a penalty of USD 15,000.
Third and any subsequent occurrence	Issuers' Primary Operations Contact receives notification by registered letter and is assessed a penalty of USD 15,000. An additional penalty of USD 15,000 is assessed for each subsequent calendar quarter that the Customer is in violation of these Rules.

After completion of a full calendar quarter without any violations, a subsequent violation is counted as a first violation.

6.15 Card Capture at the ATM

An Issuer may only transmit a Card capture command with response codes that indicate that the Card:

1. has been reported lost or stolen by a Cardholder; or
2. is determined to be fraudulent by the Issuer.

6.16 Co-Residing Applications—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

6.17 Additional Rules for Issuing—Europe and United States Regions Only

NOTE

Regional Rules on this topic appear in Chapter 16, "Canada Region," Chapter 17, "Europe Region," and in Chapter 20, "United States Region," of this rulebook.

6.18 Shared Deposits—United States Region Only

NOTE

Regional Rules on this topic appear in Chapter 20, "United States Region," of this rulebook.

6.19 Recurring Payments—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region" of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
6.1 Eligibility	A
6.2 Card Standards and Specifications	A
6.4 PIN and Signature Requirements	A
6.5 Transmitting, Processing, and Authorizing Transactions	A
6.7 Stand-In Processing Service	A
6.9 Electronic Commerce	A
6.10 Selective Authorization	B
6.12 Payment Transaction	A
6.13 Issuer Responsibilities to Cardholders	A
6.14 Fraud Reporting	A
6.15 Card Capture at the ATM	C

Chapter 7 Acquiring

This chapter contains information about acquiring requirements.

7.1 Acquirer Obligations and Activities

7.1.1 Signing a Merchant—POS and Electronic Commerce Only

NOTE

Additional regional Rules on this topic appear in Chapter 16, "Canada Region," of this rulebook.

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 Service Provider acting for or on behalf of such Acquirer.

An Acquirer must not submit for processing any Transaction resulting from the acceptance of a Card by an entity or person except pursuant to a Merchant Agreement then in effect between the Acquirer and the entity or person.

The Merchant Agreement must reflect the Acquirer's primary responsibility for the Merchant relationship and must otherwise comply with the 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 Marks continues only as long as the Merchant Agreement remains in effect. Refer to Chapter 4, "Marks," for further information about the use and display of the Marks.

NOTE

Additional regional Rules on this topic appear in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

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 Customer from chargebacks or compliance proceedings.

Each Merchant Agreement must contain a provision that sets forth payment terms agreed upon by the Customer and the Merchant, addressing when the Customer 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 Corporation.

Each Merchant Agreement with a Merchant registered as a Payment Facilitator must additionally contain the substance of Rule 7.1.3.4 of this rulebook and a provision stating that the Payment Facilitator accepts financial liability for all Transactions processed through the Interchange System on behalf of its Sub-merchants and will be responsible for the handling of all disputed Transactions, credits, and customer service-related expenses. The Merchant Agreement must provide for:

1. The Acquirer's right to terminate the Payment Facilitator; and
2. The Payment Facilitator's obligation to ensure the ongoing compliance of each of its Sub-merchants with the Standards; and
3. The Payment Facilitator's obligation to terminate the written agreement with a Sub-merchant for the conduct of activity deemed by the Payment Facilitator, it's Acquirer, or the Corporation to be in violation of the Standards.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.1.1.3 Acquirer Responsibility for Merchant and Sub-merchant Compliance

The Acquirer is responsible for ensuring that each of its Merchants complies with the Rules and technical specifications of the Corporation, and is jointly and severally liable with its Merchants or Sub-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 or Sub-merchant's compliance, such as reviewing the Merchant's deposit records and procedures for effecting Transactions. Failure by a Merchant, Sub-merchant, or Acquirer 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 or Sub-merchant and the Cardholder. Such verification must include at least all of the following:

1. Credit check, background investigations, and reference checks of the Merchant, and a check for validity of the business address and other information provided by the Merchant. If the credit check of the Merchant raises questions, the Acquirer 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.

2. Investigation of the Merchant's previous Merchant Agreements.

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

It is also recommended that the Acquirer perform an inspection of the Merchant's premises (both physical locations and Internet URLs, as applicable) and records to ensure that the Merchant has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit and other capabilities to conduct the business.

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"). The Acquirer, the Merchant, and any Sub-merchants 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.

The Corporation 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 Corporation may approve a recognized local alternative to a requirement if the alternative provides substantially the same level of protection to the Corporation.

7.1.3 Use of a Payment Facilitator

The Acquirer is liable for all acts and omissions by a Payment Facilitator and any Sub-merchant.

A Payment Facilitator may not be a Sub-merchant of any other Payment Facilitator, nor may a Payment Facilitator be a Payment Facilitator for another Payment Facilitator.

Unless otherwise approved by the Corporation, any Sub-merchant that exceeds USD 100,000 in MasterCard and Maestro annual sales may not be or continue to be a Sub-merchant and must enter into a Merchant Agreement directly with a Customer.

7.1.3.1 Responsibility for Payment Facilitator and Sub-merchant Activity

The Acquirer is responsible for the activity of the Payment Facilitator and each of its Sub-merchants, and must comply with all the following obligations related to such activity:

1. The Payment Facilitator and each of its Sub-merchants must be located within the Acquirer's licensed Area of Use as described in Rule 2.3 of this rulebook. The Acquirer must obtain an Extension of Area of Use of its license if either is located elsewhere, except as provided in Rule 2.3.2 – 3, 4 and 5 in this rulebook. The location of the Sub-merchant determines the location of a Transaction, not the location of the Payment Facilitator.
2. Settlement funds accessed by the Payment Facilitator may only be used to pay Sub-merchants.
3. An Acquirer may permit a Payment Facilitator to manage the following on behalf of the Acquirer:

    a. Verification that a Sub-merchant is a bona fide business operation, as set forth in Rule 7.1.2.1 of this rulebook;

    b. Retention of records concerning the investigation of any of its Sub-merchants, provided that such records are provided to the Acquirer immediately upon request;

    c. Payment to a Sub-merchant for Transactions by the Sub-merchants, as set forth in Rule 7.1.3.8 (4) of this rulebook;

    d. Ensuring that a Sub-merchant is supplied with materials necessary to effect Transactions as set forth in Rule 7.1.3.8 (5) of this rulebook; and

    e. Monitoring a Sub-merchant's activity on an ongoing basis to deter fraud or other wrongful activity, as set forth in Rule 7.1.3.8 (6) of this rulebook.
4. Neither the Payment Facilitator nor the Sub-merchant may require a Cardholder to waive a right to dispute a Transaction.
5. The Acquirer must ensure that all Sub-merchants are identified with the Card acceptor business code (MCC) that most closely reflects the Sub-merchant's primary business, as set forth in the *Quick Reference Booklet*. The Corporation shall have the ultimate authority to dictate the appropriate MCC if any dispute shall arise. MCC 7995 must be assigned to any Sub-merchant that sells gambling chips or other value usable for gambling, even if such sales is a minimal part of the Sub-merchant's business. (Alternatively, multiple MCCs may be used as appropriate)
6. The Acquirer must provide to the Corporation a quarterly activity report for each Sub-merchant of the Payment Facilitator that includes:

a. Sub-merchant name and location as appears in DE 43 (Card Acceptor Name/Location) of Transaction records

b. Sub-merchant "doing business as" name or URL

c. Sub-merchant MCC(s)

d. Transaction sales count and amount for each MCC

e. Transaction chargeback count and amount for each MCC

NOTE

An addition to this rule appears in Chapter 17, "Europe Region," of this rulebook.

7.1.3.2 High-Risk Payment Facilitators

A Payment Facilitator that proposes to sponsor as Sub-merchants one or more entities conducting business that may be described under any one of the following MCCs or any entity that, as a Merchant, is deemed by the Corporation to be a "High-Risk Payment Facilitator":

- Telecom merchants—MCCs 4813, 4814, 4816, and 5967
- Electronic commerce (e-commerce) adult content (videotext) merchants—MCCs 5967, 7273, and 7841
- Non–face-to-face gambling merchants—MCC 7995
- Non–face-to-face prescription drug merchants—MCC 5122 and MCC 5912
- Non–face-to-face tobacco product merchants—MCC 5993

The Corporation, in its sole discretion, may de-register a Payment Facilitator if it or any of its Sub-merchants is identified as generating excessive chargebacks or fraudulent activity or of violating any Rule or applicable law.

The Corporation reserves the right to de-register a Payment Facilitator or Sub-merchant that in the opinion of the Corporation, participates in any activity that may cause damage to the Corporation.

Each Acquirer that has entered into a Merchant Agreement with a High-Risk Payment Facilitator must ensure that the Corporation receives a monthly Sub-merchant activity report that provides the information set forth in Rule 7.1.3.1 of this rulebook.

7.1.3.3 Payment Facilitator Registration Requirement

To propose a Merchant for registration as a Payment Facilitator, the Acquirer must:

- be a Customer in good standing with the Corporation, and
- meet any and all capital requirements designated by the Corporation, and

To register a Merchant as a Payment Facilitator, the Acquirer must:

1. Submit all information and material required by the Corporation in connection with the proposed registration within sixty (60) calendar days of the registration application submission date; and
2. Ensure that the Payment Facilitator is compliant with the MasterCard Site Data Protection (SDP) Program in accordance with the implementation schedule applicable to Merchants set forth in Rule 8.10 of this rulebook. Before initiating registration, the Customer must instruct the proposed Payment Facilitator to contact the Corporation via e-mail at sdp@mastercard.com and validate its compliance with the SDP Program using the tools described in subsection 8.10.2 of this rulebook or if the proposed Payment Facilitator is not compliant, provide a Corporation-approved compliance action plan. A Corporation-approved compliance action plan does not exempt the Acquirer or its Sponsoring Principal if applicable from responsibility and liability that arises from the noncompliance of the Payment Facilitator or any of its sponsored Sub-merchants with any Standard, including those relating to the disclosure and securing of Account and Transaction data.

The Acquirer, or if an Affiliate, its Sponsoring Principal, must use the MasterCard Registration Program (MRP) system on MasterCard Connect to complete the registration procedure.

The Acquirer must receive the Corporation's written or e-mail confirmation of the Payment Facilitator's registration before the Acquirer may submit Transactions from the Payment Facilitator or any of its Sub-merchants to the Interchange System. In its sole discretion, the Corporation may approve or may reject any application for the registration of a Payment Facilitator.

To maintain the registration of a Payment Facilitator, the Acquirer must submit such information and material as may be required by the Corporation from time to time, including but not limited to a copy of the agreement between the Acquirer and Payment Facilitator. In its sole discretion, the Corporation may decline to renew the registration of a Payment Facilitator.

The Corporation will collect all registration, renewal, and any other applicable fee(s) then in effect, if any, from the Acquirer or if an Affiliate, it's Sponsoring Principal via the MasterCard Consolidated Billing System (MCBS).

If the Acquirer ceases to accept Sub-merchant Transactions from or terminates a Payment Facilitator, the Acquirer must notify the Corporation of the date and reasons for such action within one week of the decision. In its sole discretion, the Corporation may require an Acquirer to cease to accept Sub-merchant Transactions from a Payment Facilitator at any time.

7.1.3.4 Payment Facilitator Obligations

A Payment Facilitator is a Merchant and has all of the rights and responsibilities of a Merchant under the Standards.

Additionally, the Acquirer must ensure that its Payment Facilitator satisfies all of the obligations set forth in Rules 7.1.3.5 through 7.1.3.8.

7.1.3.5 Sub-merchant Screening Procedures

Before entering into, extending, or renewing an agreement with a Sub-merchant, a Payment Facilitator must verify that the entity is a bona fide business, has sufficient safeguards in place to protect Account and Transaction data permitted by the Standards to be captured from unauthorized disclosure or use, complies with applicable laws, and that each Transaction submitted by the Sub-merchant will reflect bona fide business between the Sub-merchant and a Cardholder.

In determining whether the entity is a bona fide business, the Payment Facilitator must perform a credit check, background investigations, and reference checks of the Sub-merchant, and a check for validity of the business address and other information provided by the Sub-merchant. If the credit check raises questions or does not provide sufficient information, the Payment Facilitator also should conduct a credit check of:

1. the owner, if the entity is a sole proprietor:
2. the partners, if the entity is a partnership
3. the principal shareholders, if the entity is a corporation

It is also recommended that the Payment Facilitator perform an inspection of the entity's premises or Web sites and records to ensure that it has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit and other capabilities to conduct business.

The Payment Facilitator must retain all records concerning the investigation of any entity with which it has entered into a Sub-Merchant Agreement for a minimum of two (2) years after the date the agreement is terminated or expires.

7.1.3.6 Sub-merchant Agreement

Each Payment Facilitator must enter into a written agreement with each Sub-merchant which sets forth the terms applicable to the Sub-merchants acceptance of Cards and otherwise complies with this Rule 7.1.3.6 and Rule 7.1.3.7.

The Sub-Merchant Agreement must not interfere with or lessen the right of the Payment Facilitator, the Acquirer, or the Corporation to terminate the agreement at any time. The Corporation reserves the right to restrict a Payment Facilitator from entering into a Sub-Merchant Agreement based on the business of the entity or other criteria as the Corporation deems appropriate.

7.1.3.7 Required Provisions of Sub-merchant Agreement

Each agreement between a Payment Facilitator and its sponsored Sub-merchant must contain the substance of each of the Standards set forth in the Rules, and be applicable to the nature and manner of the Sub-merchant's business. The failure of the Payment Facilitator to include the substance of any one or more of such Standards in the Sub-Merchant Agreement or the grant of a variance by the Corporation with respect to any one or more such Standards does not relieve an Acquirer from responsibility for chargebacks or compliance related to the activity of or use of the Marks by the Sub-merchant.

The Sub-Merchant Agreement must, in substance, include all of the following provisions:

1. On an ongoing basis, the Sub-merchant is promptly to provide the Payment Facilitator with the current address of each of its offices, all "doing business as" (DBA) names used by the Sub-merchant, and a complete description of goods sold and services.
2. In the event of any inconsistency between any provision of the Sub-Merchant Agreement and the Standards, the Standards will govern.
3. The Payment Facilitator is responsible for the Card acceptance policies and procedures of the Sub-merchant, and may require any changes to its Web site or otherwise that it deems necessary or appropriate to ensure that the Sub-merchant remains in compliance with the Standards governing the use of the Marks.
4. The Sub-Merchant Agreement automatically and immediately terminates if the Corporation de-registers the Payment Facilitator or if the Payment Facilitator's Acquirer ceases to be a Customer for any reason or if such Acquirer fails to have a valid License with the Corporation to use any Mark accepted by the Sub-merchant.
5. The Payment Facilitator may, at its discretion or at the direction of its Acquirer or the Corporation, immediately terminate the Sub-Merchant Agreement for activity deemed to be fraudulent or otherwise wrongful by the Payment Facilitator, its Acquirer, or the Corporation.
6. The Sub-merchant acknowledges and agrees:

    a. to comply with all applicable Standards, as amended from time to time;

    b. that the Corporation is the sole and exclusive owner of the Marks;

    c. not to contest the ownership of the Marks for any reason;

    d. the Corporation may at any time, immediately and without advance notice, prohibit the Sub-merchant from using any of the Marks for any reason;

    e. the Corporation has the right to enforce any provision of the Standards and to prohibit the Sub-merchant and/or its Payment Facilitator from engaging in any conduct the Corporation deems could injure or could create a risk of injury to the Corporation, including injury to reputation, or that could adversely affect the integrity of the Interchange System,

the Corporation's confidential information as defined in the Standards, or both; and

f. the Sub-merchant will not take any action that could interfere with or prevent the exercise of this right by the Corporation.

The Sub-Merchant Agreement must not contain any terms that conflict with any Standard.

7.1.3.8 Obligations as Sponsor of Sub-merchants

A Payment Facilitator must fulfill all of the following obligations with respect to each of its Sub-merchants.

1. Submit Valid Transactions

   The Payment Facilitator must submit to its Acquirer records of valid Transactions submitted by a Sub-merchant and involving a bona fide Cardholder. The Payment Facilitator must not submit to its Acquirer any Transaction that the Payment Facilitator or the Sub-merchant knows or should have known to be fraudulent or not authorized by the Cardholder, or that either knows or should have known to be authorized by a Cardholder colluding with the Sub-merchant for a fraudulent purpose. For purposes of this Rule, the Sub-merchant is deemed to be responsible for the conduct of its employees, agents, and representatives.

2. Sub-merchant Compliance with the Standard

   The Payment Facilitator is responsible for ensuring that each of its Sub-merchants complies with the Standards, including but not limited to the Card acceptance requirements set forth in Rule 7.1.8 of this rulebook. The Payment Facilitator must take such actions that may be necessary or appropriate to ensure the Sub-merchant's ongoing compliance with the Standards.

3. Maintaining Sub-merchant Information

   The Payment Facilitator must maintain, on an ongoing basis, the names, addresses, and URLs if applicable of each of its Sub-merchants. The Acquirer must ensure that the Payment Facilitator promptly supplies the Corporation with any such information upon request.

4. Payments to Sub-merchants

   Each Payment Facilitator must pay each Sub-merchant for all Transactions the Payment Facilitator submits to its Acquirer on the Sub-merchant's behalf. This obligation is not discharged with regard to a Transaction until the Sub-merchant receives payment from the Payment Facilitator with which the Sub-merchant has entered into an agreement, notwithstanding any payment arrangement between the Sub-merchant and the Payment Facilitator or between the Payment Facilitator and its Acquirer. A Sub-Merchant Agreement may provide for a Payment Facilitator to withhold amounts for chargeback reserves or similar purposes.

5. Supplying Materials to Sub-merchants

Each Payment Facilitator must regularly ensure that each of its Sub-merchants is provided with all materials necessary to effect Transactions in accordance with the Standards and to signify Maestro acceptance. These materials may include sales slips, credit slips, terminals, authorization services, Maestro acceptance decals, signage, and the like.

6. Sub-merchant Monitoring

   Each Payment Facilitator must monitor on an ongoing basis the activity and use of the Marks of each of its Sub-merchants for the purpose of deterring fraudulent and other wrongful activity and to ensure ongoing compliance with the Standards. For purposes of this Rule, the minimum Merchant monitoring Standards set forth in this rulebook apply with respect to Sub-merchants.

7. Sub-merchant Identification to Cardholders

   Each Payment Facilitator must ensure that, if the Cardholder is linked to a Payment Facilitator's Web site from a Sub-merchant's Web site for payment, the name of the Payment Facilitator must appear in DE 43 (Card Acceptor Name/Location), subfield 1 (Card Acceptor Name) in conjunction with the name of the Sub-merchant. If the Cardholder accesses the Payment Facilitator's Web site directly, and its name is visible to the Cardholder throughout the Transaction from selection of goods and/or services to the completion of the checkout process, then the Payment Facilitator's name may appear in DE 43 without the name of the Sub-merchant.

7.1.4 ATM Owner Agreement

Each Acquirer must have a written agreement (the "ATM Owner Agreement") with the owner of every ATM from which it intends to acquire Transactions, whether such Transactions are submitted to the Acquirer by the ATM owner, or through a Service Provider acting for or on behalf of such Acquirer. If an Acquirer uses an MSP, the Acquirer must itself execute a written agreement directly with each ATM owner.

The ATM Owner Agreement must be updated as appropriate to reflect the services provided by the ATM owner and may not contradict, or be inconsistent with, the Standards.

The Acquirer must maintain the executed version of the ATM Owner Agreement and must make it available to the Corporation upon request.

7.1.4.1 Required Information

The ATM Owner Agreement must include the following:

1. The complete name and address of the ATM owner (or principals of the business if the ATM owner is a corporation, partnership, or limited liability company).
2. The complete address of the ATM location, if the ATM location address is different from the address of the ATM owner.
3. The ATM owner's legal status (for example, corporation, partnership, sole proprietor, non-profit, other), and the applicable Federal Taxpayer Identification Number (TIN), Federal Employer Identification Number (FEIN) or Social Security Number (SSN), or other equivalent government registration identifiers appropriate to the ATM owner's country of operation.
4. The legal name, and if applicable the "Doing Business As" (DBA) name, of the ATM location.
5. The complete name and address of any Third Party Processor (TPP) performing services for, or otherwise associated with, the ATM owner.
6. The complete name and address of any entity, other than the ATM owner, that receives revenue as a result of the use, lease, placement, and/or maintenance of the ATM.

7.1.4.2 Required Provisions

The ATM Owner Agreement must reflect the Acquirer's responsibility for establishing all management and operating policies relating to its ATM transaction acquiring programs and must not include any provision that limits, or attempts to limit, the Acquirer's responsibility for such programs. The ATM Owner Agreement must, in substance, include all of the following provisions:

1. The ATM owner received, understands, and agrees to comply with all Standards that apply to the nature and manner of the ATM owner's business as that business relates to the ownership and/or deployment of an ATM.
2. On an ongoing basis, and in no event less than quarterly, the ATM owner is promptly to provide the Acquirer with all information for each of its ATM locations as required by the Corporation to maintain its Location Administration Tool (LAT) (formerly the ATM Directory/ATM Locator), including but not limited to:
   - Location Name
   - Address
   - Terminal ID
3. In the event of any inconsistency between any provision of the ATM Owner Agreement and the Standards, the Standards shall govern.
4. The ATM Owner Agreement automatically terminates if the Acquirer ceases to be a Customer for any reason. The Corporation retains the right to require

that the Acquirer terminate the ATM Owner Agreement if the Corporation determines that any ATM owner appears not to be qualified for any reason.

5. The ATM owner acknowledges that the Corporation is the sole and exclusive owner of the Marks and agrees that the ATM owner will not contest the ownership of the Marks for any reason whatsoever. The Corporation may at any time, immediately and without advance notice, prohibit the ATM owner from using any of the Marks for any reason.
6. The ATM owner acknowledges and agrees that the Corporation has the right to enforce any provision of the Standards and to prohibit any ATM owner conduct that may injure or may create a risk of injury to the Corporation, including injury to reputation, or that may adversely affect the integrity of the Corporation's core payment systems, information, or both. The ATM owner must agree not to take any action that might interfere with, or prevent exercise of, this right by the Corporation.

7.1.4.3 Before Entering into an ATM Owner Agreement with an ATM Owner

Acquirer must verify that the ATM owner is a bona fide business and that the ATM owner has sufficient safeguards in place to protect Cardholder and Transaction information from unauthorized disclosure and/or use.

In determining whether the ATM owner is a bona fide business, the Acquirer must verify, at a minimum, that all of the following have been completed:

1. Credit check and background investigations of the ATM owner. If the credit check of the ATM owner raises questions or does not provide sufficient information, the Acquirer should also conduct a credit check of:
   a. the owner, if the ATM owner is a sole proprietor;
   b. the partners, if the ATM owner is a partnership;
   c. the principal shareholders, if the ATM owner is a corporation; or
   d. the owners, if the ATM owner is a limited liability company.
2. Confirmation that all ATMs claimed by the ATM Owner exist and are operational.
3. Verification of the location and condition of all ATMs deployed by the ATM Owner.

The Acquirer must have records to ensure that the ATM owner has the proper facilities, equipment, inventory, agreements, and personnel required and, if necessary license or permit, and other capabilities to conduct business as that business relates to the ownership and/or deployment of an ATM.

The Acquirer must retain all records concerning the investigation of any ATM owner with which it has entered into an ATM Owner Agreement for a minimum of two years after the date the agreement is terminated or expires.

7.1.5 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 Customers, 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 Corporation. The Acquirer must perform tests, both initially and on an on-going basis to ensure compliance with this Rule.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.1.6 Certification Process

Before acquiring Transactions, Acquirers must follow the procedures for testing and certification of their connection(s) to the Interchange System, as agreed by the Corporation from time-to-time and published to Customers. Thereafter, Acquirers must upgrade their connections as necessary, to ensure continued compatibility with the current technical specifications of the Corporation, and must certify such upgrade, if required.

7.1.7 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 to the Interchange System, in accordance with the applicable Standards. Refer to Chapter 9, "Processing Requirements," for additional information.

In addition to all other message format requirements, Acquirers must transmit within each Transaction record the Terminal location description, the name of the Customer that owns or sponsors the ATM, the Terminal or Merchant address where the ATM is located, and the Terminal identification (which must be unique) within each Transaction record. For additional information refer to the technical specifications.

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 17, "Europe Region," of this rulebook.

7.1.8 Card Acceptance Requirements

Each Acquirer must ensure that:

1. it actively promotes the Corporation;
2. the 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;
3. the Marks are displayed at least in the same size and place as any competing acceptance brand;
4. all valid Cards are honored without discrimination when properly presented by Cardholders at any POI Terminal displaying the 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;
5. a Merchant does not require, or post signs indicating that it requires a minimum or maximum Transaction amount to accept a valid Card;
6. 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;
7. 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, and an acknowledgement file confirming that such files are input and available for use has been sent to the Corporation;
8. any Card that conforms with the encoding Standards is accepted as a valid Card;
9. 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;
10. all required Transaction types are supported, as described in Chapter 9, "Processing Requirements," of this rulebook;
11. all valid Transactions are accepted and processed in accordance with the Standards;
12. 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 "PAN Truncation Requirements" later in this chapter for further information.);

13. 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.

NOTE

Rule variations on this topic appear in Chapter 21, "Maestro *PayPass*," of this rulebook.

7.1.9 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, "Customer Obligations," for further information.

During the required retention period for POS Transactions, Acquirers must produce a copy of a Transaction receipt, upon request.

7.1.10 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.

7.1.11 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 Corporation.

7.1.12 Management Information

Acquirers must provide agreed management information as required by the Rules with respect to Licensing and Activities of the Corporation.

7.1.13 Quality Assurance

From time-to-time, the Corporation 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 Corporation from time-to-time, and published to Customers.

7.1.14 Currency Conversion

At its option, an Acquirer or Merchant may offer currency conversion at any POI Terminal.

If the Acquirer or Merchant offers currency conversion at a POI Terminal, it must:

- Before initiation of the Transaction, (i) clearly and conspicuously inform the Cardholder that the Cardholder has the right to choose the method of currency conversion to be applied to the Transaction (for example, by the Acquirer or Merchant, or by the Corporation); and (ii) obtain the Cardholder's choice of currency conversion method;
- If the Cardholder chooses the option of currency conversion by the Acquirer or Merchant, clearly and conspicuously inform the Cardholder of the same elements as are set forth in Rule 7.15.5 of this manual, and obtain the Cardholder's consent to those elements before completion of the Transaction.

The pre-conversion currency and amount must be provided in DE 54 of Financial Transaction/0200 messages and First Presentment/1240 messages in accordance with the technical specifications.

Please refer to Rule 7.15.5 of this manual for the Transaction receipt requirements applicable to currency conversion by the Acquirer.

No specific currency conversion method may be implemented as the default option. As an exception to the preceding requirement, when POI currency conversion is offered on the Internet a currency conversion option may be pre-selected.

Before offering POI currency conversion at ATMs or unattended POS Terminals, the Acquirer must submit the proposed screen messages and a sample receipt for approval by the Corporation. Alternatively, the Acquirer may implement screen messages and a receipt as shown in Appendix D without advance approval.

Screen messages at ATMs or unattended POS terminals must not require the Cardholder to choose between "YES" and "NO" when choosing the currency. Indirect means, such as the colors red and green, must not be used to influence the cardholder's choice.

At attended POS Terminals that require the cardholder to choose between "YES" and "NO," the Merchant must verbally explain the offer to the Cardholder before presenting it on the POS Terminal.

If the Cardholder chooses currency conversion by the Corporation, the Acquirer must present the Transaction for clearing in the currency in which goods, services, or both, were priced or in the currency that was dispensed to the Cardholder.

The same currency conversion method must be used for a refund as was used for the corresponding purchase Transaction.

7.1.15 Information to Merchants—European Economic Area Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.1.16 Acquirer Host System Requirements

NOTE

A regional Rule on this topic appear in Chapter 20, "United States Region," of this rulebook.

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 Rule 7.1, on an ongoing basis, each Acquirer must:

1. 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 Marks;
2. monitor its Merchants' compliance with the Rules and technical specifications of the Corporation, including checking for and testing out Merchant contact details. If requested by the Corporation, 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;
3. acquire all Transactions properly presented to it from each of its Merchants on such terms as set forth in the Merchant Agreement between them;

4. 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;
5. be satisfied that the Merchant is able to support the fulfillment of the products and/or services to be marketed;
6. ensure that the Merchant has procedures and resources to handle Cardholder inquiries and to support refunds, where necessary;
7. provide the respective Merchant/outlet descriptions within each Transaction record;
8. ensure that the Merchant assigns an account for the crediting and debiting of Transactions, and for the debiting of items charged back;
9. 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 Customer, notwithstanding any Customer payment arrangement, including any such arrangement between an Affiliate and its Principal. An Acquirer may, by agreement of the Merchant, withhold amounts for chargeback reserves or similar purposes;
10. ensure that each Merchant, and before a Data Storage Entity (DSE) is permitted to access Card data, Transaction data, or both;
    a. informs the Acquirer of the identity of any DSE that the Merchant intends to afford access to such data and provides the Acquirer the opportunity to approve or disapprove of the proposed use of the DSE, and
    b. causes the DSE to complete the registration procedures described in Rule 14.6 of this rulebook;
11. 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;
12. ensure that Merchants immediately notify the Acquirer of an Account compromise. Refer to Rule 7.2.1 for additional information;
13. 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 Corporation, or in response to a government request.

NOTE

Additional regional Rules and regional Rule variations on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.2.1 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, or as the Corporation has expressly permitted in writing.

NOTE

Additional regional Rules on this topic appear in Chapter 16, "Canada Region," and a regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

7.2.2 Merchant Noncompliance

The Corporation will notify an Acquirer if the Acquirer or the Acquirer's Merchant fails to comply with the Rules.

The Corporation may require action to eliminate the deficiencies, require the Acquirer to suspend or discontinue Corporation Activities with the Merchant concerned, or levy noncompliance assessment fees.

7.2.3 Refinancing of Previously Existing Debt and/or Payment of Bad Debts—Asia/Pacific Region Only

NOTE

Regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," of this rulebook.

7.2.4 Additional Acquiring Requirements—South Asia/Middle East/Africa Region Only

NOTE

Regional Rules on this topic appear in Chapter 19, "South Asia/Middle East/Africa Region," of this rulebook.

7.3 Additional Acquirer Obligations and Activities for Terminals

In addition to the requirements documented in Rules 7.1.3 through 7.1.14, on an ongoing basis Acquirers must:

1. determine the supplier, manufacturer, and model of each Terminal; and
2. provide the Corporation with current and accurate information regarding its Terminals, by updating quarterly the Location Administration Tool (LAT) located on MasterCard Connect. Refer to Chapter 9, "Processing Requirements," for further information.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook

7.4 Acquiring Electronic Commerce Transactions

An electronic commerce Transaction must not be effected using Maestro *PayPass* contactless payment functionality.

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 requirements set forth in Rule 2.3 of this rulebook.

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 Customers as to a Merchant's location may be referred to the Corporation for resolution.

NOTE

A regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

7.4.1 Acquirer Responsibilities: Electronic Commerce Transactions

In addition to the requirements documented in Rules 7.1, 7.2 and 7.4, Acquirers must ensure that all Merchant sites that accept electronic commerce Transactions:

1. clearly display the Marks on the Web site. The method and size used to display the 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;
2. are capable of accepting PANs between thirteen (13) and nineteen (19) digits in length;
3. support the passing of authentication data in the UCAF;
4. support 3D Secure Merchant Plug-in, and are capable of handling Transactions within a 3D Secure environment;
5. provide a set of "help" functions to help Cardholders that have not yet been enabled by their Issuers for transacting via the Internet;
6. 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;
7. 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. Refer to the *MasterCard SecureCode Acquirer Implementation Guide* for more information.

NOTE

Additional regional Rules and a regional Rule variation on this topic appear in Chapter 18, "Latin America and the Caribbean Region," of this rulebook, and an additional Rule appears in Chapter 19, "South Asia/Middle East/Africa Region," and Chapter 20, "United States Region," of this rulebook.

7.4.1.1 Merchant Requirements: Electronic Commerce Transactions

Each Merchant must:

1. clearly display a mailing address, and a contact telephone number or
2. 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;

3. support MasterCard *SecureCode*;
4. have the capability to accept PANs between thirteen (13) and nineteen (19) digits in length;
5. 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;
6. display a receipt page, after the Cardholder confirms a purchase. The display of the receipt on the screen must be printable;
7. 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;
8. 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;
9. 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.;
10. 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;
11. 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 Corporation. For more information, refer to the *MasterCard SecureCode—Merchant Implementation Guide*.

NOTE

A regional Rule appears on this topic in Chapter 19, "South Asia, Middle East/Africa Region," of this rulebook. Rule variations on this topic appear in Chapter 20, "United States Region," of this rulebook.

7.5 Acquiring Payment Transactions

1. Only Acquirers and Merchants approved and registered by the Corporation to effect Payment Transactions may do so.

2. Acquirers must always submit a postable authorization request to the receiving Issuer for all Payment Transactions.
3. The Acquirer or Merchant must present the Payment Transaction on or before the date agreed to with the recipient Cardholder.
4. 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.
5. In a dual message environment, Acquirers must submit a clearing message to the Interchange System within twenty-four (24) hours of the authorization request.
6. 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.
7. 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 Corporation will also, from time to time, perform audits on these Merchants to ensure that they are compliant with this and all other requirements.
8. 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.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," of this rulebook.

7.5.1 Customer Registration Procedures for Payment Transactions

A Payment Transaction may be submitted for processing, only by Customers or Merchants that are registered by the Corporation. When determining whether to register a Customer or Merchant, the Corporation will consider several factors, including but not limited to, the following:

1. Customer compliance with the Rules and systems requirements;

2. 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);
3. appropriate Cardholder experience (for example, Cardholder procedures for inquiries and disputes); and
4. Customer financial control and risk management procedures.

The Corporation will monitor programs on an ongoing basis. In its sole discretion, the Corporation may rescind its approval and Customer or Merchant registration at any time.

7.6 Acquiring *MoneySend* Payment Transactions

1. Only Acquirers approved and registered by the Corporation to effect MasterCard® *MoneySend*™ Payment Transactions may do so.
2. Funds for the MasterCard *MoneySend* Payment Transaction must be deemed collected and in the control of the Acquirer before the MasterCard *MoneySend* Payment Transaction is submitted for authorization.
3. The Acquirer must submit an authorization request to the Issuer for each MasterCard *MoneySend* Payment Transaction.
4. The Acquirer must not aggregate two (2) or more MasterCard *MoneySend* Payment Transactions into a single Payment Transaction. Conversely, the Acquirer may not divide one MasterCard *MoneySend* Payment Transaction into two or more MasterCard *MoneySend* Payment Transactions. Each MasterCard *MoneySend* Payment Transaction must be authorized, cleared and settled distinctly and separately.
5. In a dual message environment, Acquirers must submit a clearing message to the Interchange System within one (1) calendar day of the Issuer's approval of the authorization request.
6. In a dual message environment, the Acquirer must ensure that the amount of the MasterCard *MoneySend* Payment Transaction in the clearing message matches the amount in the authorization request.
7. Any requests by the Acquirer to correct a clerical error will be approved or rejected at the discretion of the Issuer. Refer to Rule 9.8.8 of this rulebook for additional information.
8. An Acquirer that offers the option to use the MasterCard *MoneySend* Payment Transaction to send funds to a recipient must:

    a. establish procedures to verify and authenticate the sender's identity; and

    b. set forth the details of the MasterCard *MoneySend* Payment Transaction on the sender's statement, including the amount of the MasterCard *MoneySend* Payment Transaction and the date on which the funds were withdrawn from the sender's account.

9. The Acquirer must not effect a MasterCard *MoneySend* Payment Transaction in order to transfer funds to a Merchant, a commercial entity, or a commercial Card.

NOTE

Regional Rule variations on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.7 Acquiring Mobile Remote Payment Transactions

Acquirers that want to acquire Mobile Remote Payment Transactions must register with the Corporation.

7.7.1 Issuer Domain Mobile Remote Payment Transactions

Acquirers must support the passing of the data in UCAF with the Accountholder Authentication Value (AAV) to the Interchange System for Issuer Domain Mobile Remote Payment Transactions. Refer to the *Mobile Remote Payments Program Guide* for additional information.

Acquirers must provide implementation and registration for Merchants or delegate a specific implementation and registration function to Corporation-approved provider. Refer to the *Mobile Remote Payments Program Guide* for additional information.

7.7.1.1 Acquirer Responsibilities: Issuer Domain Mobile Remote Payment Transactions

In addition to the requirements documented in Rules 7.1 and 7.2, Acquirers must ensure that all Merchants registered for the Mobile Remote Payment program:

1. Are capable of accepting PANs between thirteen (13) and nineteen (19) digits in length;
2. Comply with the requirements set forth in the *Mobile Remote Payments Program Guide*.

7.7.1.2 Merchant and/or Service Manager Requirements: Issuer Domain Mobile Remote Payment Transactions

Acquirers must ensure that each Merchant and/or Service Manager must:

1. Provide clear instructions on how to obtain a mailing address, and a contact telephone number or e-mail address, for Cardholder queries resulting from Issuer Domain Mobile Remote Payment Transactions. This information may be provided in the confirmation message, 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;
2. Have the capability to accept PANs between thirteen (13) and nineteen (19) digits in length;
3. Provide a function for Cardholders to confirm a Mobile Remote Payment Transaction. This confirmation function must be provided before the sale has been completed and any charges levied;
4. Provide a confirmation of payment message after the Cardholder confirms the Mobile Remote Payment Transaction. The confirmation message must include Transaction date, Transaction amount, Merchant reference, unique Transaction reference, and contact details for Cardholder inquiries;
5. Ensure that information provided on any electronic acknowledgement of the Cardholder's order is in compliance with all other requirements for a Mobile Remote Payment Transaction receipt. Refer to the *Mobile Remote Payments Program Guide* for additional information.

7.7.2 Acquirer Domain Mobile Remote Payment Transactions

Acquirers that offer Acquirer Domain Mobile Remote Payment Transaction programs to Merchants and Cardholders must register with the Corporation. Refer to the *Mobile Remote Payments Program Guide* for additional information.

An Acquirer may use a Service Manager to provide Mobile Remote Payment Program Service. Acquirers using a Service Manager to participate in a Mobile Remote Payment Program must register each Service Manager proposed to provide Mobile Remote Payment Program Service as a Third Party Processor, as set forth in Rule 14.6 of this rulebook.

The Acquirer must ensure the Service Manager complies with all applicable Standards, including the branding requirements and the security requirements and guidelines for Mobile Remote Payments. Refer to the *Mobile Remote Payments Program Guide* for additional information.

Acquires must provide implementation and registration for Merchants and Cardholders or delegate a specific implementation and registration function to the Service Manager. Refer to the *Mobile Remote Payments Program Guide* for additional information.

7.7.2.1 Acquirer Responsibilities: Acquirer Domain Mobile Remote Payment Transactions

In addition to the requirements documented in Rules 7.1 and 7.2., Acquirers must ensure that all Merchants and Services Mangers registered for the Acquirer Domain Mobile Remote Payment program:

1. are capable of accepting PANs between thirteen (13) and nineteen (19) digits in length, and
2. comply with the requirements set forth in the *Mobile Remote Payments Program Guide*.

7.7.2.2 Merchant and/or Service Manager Requirements: Acquirer Domain Mobile Remote Payment Transactions

Acquirers must ensure that each Merchant and/or Service manager:

1. Provide clear instructions on how to obtain a mailing address, and a contact telephone number or e-mail address, for Cardholder queries resulting from Acquirer Domain Mobile Remote Payment Transactions. This information may be provided in the confirmation message, 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 Mobile Remote Payment Transaction was performed;
2. Have the capability to accept PANs between thirteen (13) and nineteen (19) digits in length;
3. Provide a function for Cardholders to confirm an Acquirer Domain Mobile Remote Payment Transaction This confirmation must be provided before the sale has been completed and any charged levied;
4. Provide a confirmation of payment message after the Cardholder confirms the Acquirer Domain Mobile Remote Payment Transaction. The confirmation message must include the Transaction date, Transaction amount, Merchant reference, unique Transaction reference, and contact details for Cardholder inquiries; and
5. Ensure that information provided on any electronic acknowledgement of the Cardholder's order is in compliance with all other requirements for a Mobile Remote Payment Transaction receipt. Refer to the *Mobile Remote Payments Program Guide* for additional information.

7.8 Eligible POI Terminals

The following types of terminals are eligible to be POI Terminals as applicable:

1. any ATM that is owned, operated or controlled by a Customer, and that is capable of complying with all of the applicable provisions of the Rules, and the regulations, policies and technical specifications of the Corporation;

2. any ATM that is owned, operated or controlled by an entity that is ineligible to be a Customer, provided that such ATM is connected to the Interchange System by a Principal or Affiliate and is capable of complying with all the applicable provisions of the Rules, and the regulations, policies and technical specifications of the Corporation. Refer to Chapter 14, "Service Providers," for additional information;
3. 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 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 Corporation. Refer to Rule 7.1.1 as set forth in this chapter;
4. any other type of terminal which the Corporation may authorize.

All POI Terminals must be identified by the appropriate Marks pursuant to the Rules, and the regulations, policies and Identity Standards of the Corporation.

7.8.1 Ineligible Terminals

All terminals that dispense scrip must be disconnected from the Interchange System.

Acquirers are prohibited from sponsoring into the Corporation any terminals that dispense scrip.

7.9 POS Terminal and Terminal Requirements

All eligible POS Terminals and Terminals must:

1. perform Transactions only after receiving authorization from the Issuer or from the Chip Card;
2. read and transmit all track 2 data encoded on the Card's magnetic stripe for authorization;
3. provide operating instructions in English as well as the local language;
4. ensure privacy of PIN entry to the Cardholder;
5. 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
6. prevent additional Transactions from being entered into the system while a Transaction is being processed.

It is strongly recommended that all POS Terminals and Terminals be chip capable.

NOTE

Regional Rule variations on this topic appear in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook, and Rule variations on this topic appear in Chapter 21, "Maestro *PayPass*," of this rulebook.

7.9.1 Card Reader

POS Terminals and Terminals must have a magnetic stripe reader capable of reading track 2 data encoded on Cards.

NOTE

A Rule variation on this topic appears in Chapter 21, "Maestro *PayPass*," of this rulebook.

7.9.2 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 15, "Asia/Pacific Region," Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook, and a Rule variation on this topic appears in Chapter 21, "Maestro *PayPass*," of this rulebook.

7.9.3 PIN Entry Device

PIN entry devices must:

1. have a numeric keyboard to enable the entry of PINs;
2. have an 'enter key' function, in order to indicate the completion of the entry of a variable length PIN;
3. accept PINs having four (4) to six (6) numeric characters. Note: The Corporation strongly recommends that PINs up to twelve (12) characters be supported.

Regional Rule variations on this topic appears in Chapter 16, "Canada Region," and Chapter 20, "United States Region," of this rulebook, and a Rule variation on this topic appears in Chapter 21, "Maestro *PayPass*," of this rulebook.

7.9.4 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.

1. 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."
2. 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 17, "Europe Region," of this rulebook.

7.9.5 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.

7.9.6 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

An additional regional Rule on this topic appears in Chapter 20, "United States Region," of this rulebook.

7.9.7 Card Authentication—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.10 Hybrid POS Terminal and Hybrid Terminal Requirements

In addition to the requirements listed in Rule 7.9 of this rulebook, all hybrid POS Terminals and hybrid Terminals must:

1. read required data from the chip when present in Chip Cards, and either transmit or process, as appropriate, all required data for authorization processing;
2. perform the Transaction using the EMV chip;
3. be capable of performing fallback procedures when the Transaction cannot be completed using chip technology because of a technical failure;
4. comply with the acceptance requirements set forth in the chip technical specifications, as published from time to time by the Corporation;
5. request a cryptogram for all chip-read Transactions; if the transaction is approved, transmit an application cryptogram and related data.

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.

A chip-capable POS Terminal or Terminal that does not satisfy all of the requirements to be a Hybrid POS Terminal or Hybrid Terminal, respectively, is deemed by the Corporation to be a magnetic stripe-only POS Terminal or Terminal, respectively, and must be identified in Transaction messages as such.

NOTE

For Europe region Rules about technical fallback at POS Terminals, ATMs, and PIN-Based In-Branch Terminals, refer respectively to Rules 7.11.1, 7.12.1. and 7.13.1 in Chapter 17, "Europe Region," of this rulebook.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

7.10.1 Chip Liability Shift—Canada and Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 16, "Canada Region," and Chapter 17, "Europe Region," of this rulebook.

7.11 Additional Requirements for POS Terminals

In addition to the requirements listed in Rule 7.9 of this rulebook:

1. each Merchant is responsible for the maintenance arrangements of its POS Terminals, unless the Acquirer undertakes this function; and

2. 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.

It is strongly recommended that all POS Terminals read and act on extended service codes.

NOTE

An additional regional Rule on this topic appears in Chapter 15, "Asia/Pacific Region," and Chapter 20, "United States Region," of this rulebook.

7.11.1 Additional Requirements for Hybrid POS Terminals

In addition to the requirements listed in Rules 7.9 POS Terminal and Terminal Requirements, 7.10 Hybrid POS Terminal and Hybrid Terminal Requirements, and 7.11 Additional Requirements for POS Terminals of this rulebook, hybrid POS Terminals must:

1. support both online and offline PIN as the CVM. On a country-by-country basis, the Corporation may permit Acquirers to, at a minimum, support offline PIN as the CVM as outlined in Rule 6.4.3 of this rulebook.
2. perform the following risk management functions: floor limit and Card velocity checking. For offline Transactions, refer to the *Quick Reference Booklet* for information regarding floor limits for POS Terminals. Transactions above the floor limit programmed in the POS Terminal must be routed online to the Issuer, as indicated by the authorization request cryptogram (ARQC).

Hybrid POS Terminals that connect to an acquiring network must support online mutual authentication (OMA) and script processing.

Hybrid POS Terminals are not required to support offline Transactions. However, any hybrid POS Terminals that support offline Transactions must identify all offline Transactions as such to the Issuer when submitting the Transactions for clearing and settlement.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

7.11.2 Hybrid POS Terminal CAM Policy

All hybrid POS Terminals must, at a minimum, support online authorization. The Corporation strongly recommends that all hybrid POS Terminals be capable of both online and offline authorization.

If an Acquirer chooses to use both online and offline authorization, that Acquirer's hybrid POS Terminals installed on or after 1 January 1999 must support offline SDA CAM, offline DDA CAM, and, effective 1 January 2011, offline CDA CAM. An Acquirer's hybrid POS Terminal installed before 1 January 1999 must support offline SDA CAM and, at the Acquirer's option, may support offline DDA CAM.

If an Acquirer chooses to use only online authorization that Acquirer's hybrid POS terminals may optionally support offline CAM. However, if an Acquirer that uses only online authorization supports offline CAM at its hybrid POS terminals, it must support both offline SDA CAM, offline DDA CAM, and effective 1 January 2011, offline CDA CAM.

If offline SDA, DDA, or CDA CAM is performed and fails, the Issuer may still process the Transaction via online CAM, if available. If offline CAM fails at any hybrid POS Terminal and the Chip Card does not request online processing, the Transaction must be declined.

For chip Transactions, Cards must be validated in accordance with the requirements described in the chip technical specifications as published from time to time by the Corporation.

Refer to Chapter 9, "Processing Requirements," for information about offline processing.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.11.2.1 Hybrid POS Terminal Offline PIN Policy

Any new hybrid POS Terminals that support offline PIN verification must support both clear text PIN and enciphered PIN. This mandate applies to all EMV-capable hybrid POS Terminals which support offline PIN that are submitted for type approval on or after 1 January 2002.

This mandate applies to all other existing EMV-capable hybrid POS Terminals that support offline PIN.

7.12 Additional Requirements for ATMs

In addition to the requirements listed in Rule 7.9 of this rulebook, all ATMs must:

1. permit the Cardholder to obtain the equivalent of USD 100 in the currency in use at the Terminal per Transaction, subject to authorization of the Transaction by the Issuer;
2. process each Transaction in the currency dispensed by the ATM during that Transaction. ATMs may process Transactions in other currencies only if done in accordance with the currency conversion requirements set forth in Rule 7.1.14 of this rulebook, except that a withdrawal of foreign currency

may be processed in the issuing currency of the Card if it is the same as the currency of the country where the ATM is located.

The amount of currency dispensed, Transaction amount, and conversion rate must be shown on the screen before the Cardholder completes the Transaction and included on the Transaction receipt.

3. contain keyboards that display and allow entry of Arabic digits 0 through 9, inclusive. Note: It is recommended that keyboards permit alphanumeric input with letter-number combinations as follows:

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

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

NOTE

A regional Rule variation on this topic appears in Chapter 16, "Canada Region," and Chapter 20, "United States Region," of this rulebook.

7.12.1 Additional Requirements for Hybrid ATMs

In addition to the requirements listed in Rules 7.9, 7.10 and 7.12 of this rulebook, hybrid ATMs must:

1. be EMV-compliant;
2. support online PIN as the CVM.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.12.1.1 Hybrid ATM CAM Policy

For chip Transactions, Cards must be validated in accordance with the requirements described in the chip technical specifications manual as published from time to time by the Corporation.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," of this rulebook.

7.13 Additional Requirements for PIN-based In-Branch Terminals

In addition to the requirements listed in Rule 7.9 of this rulebook, PIN-based In-Branch Terminals must:

1. receive written approval from the Corporation, before having access to the Interchange System;
2. accept all Cards. Branches offering the service must display the Marks on the door or window, and at the counter where the service is provided;
3. clearly describe by receipt, screen information, or both the action taken in response to a Cardholder's request. Note: It is recommended that the branch address be printed on the receipt as well;
4. have at least single-line screens that provide a minimum screen width of sixteen (16) characters. Note: Multi-line screens and screens with greater width than sixteen (16) characters are recommended;
5. permit the Cardholder to obtain the equivalent of USD 200, in local currency per Transaction, subject to authorization of the Transaction by the Issuer. PIN-based In-Branch Terminals are permitted to dispense currency other than the local currency, provided the Cardholder is informed of the currency that will be dispensed before the Transaction is made, and, if a receipt is provided, it must identify the currency dispensed.
6. process Transactions in the currency dispensed by the PIN-based In-Branch Terminal if the PIN-based In-Branch Terminal is a new, replacement or refurbished PIN-based In-Branch Terminal deployed on or after 1 January 2007. Effective 1 November 2007, all PIN-based In-Branch Terminals must process Transactions in the currency dispensed by the PIN-based In-Branch Terminal. PIN-based In-Branch Terminals may process Transactions in other currencies if done in accordance with the currency conversion requirements set forth in Rule 7.1.14 of this rulebook.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.13.1 Additional Requirements for Hybrid PIN-based In-Branch Terminals

In addition to the requirements listed in Rules 7.9, 7.10 and 7.13 of this rulebook, hybrid PIN-based In-Branch Terminals must comply with the requirements set forth in Rule 7.12.1 of this rulebook.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.13.1.1 Hybrid PIN-based In-Branch Terminal CAM Policy

For chip Transactions, Cards must be validated in accordance with the requirements described in the chip technical specifications as published from time to time by the Corporation.

NOTE

An additional regional Rule on this topic appears in Chapter 17, "Europe Region," of this rulebook.

7.14 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 and a Rule variation on this topic appear in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

7.15 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 17, "Europe Region," of this rulebook, and a Rule variation on this topic appears in Chapter 21, "Maestro *PayPass*" of this rulebook.

7.15.1 Receipt Contents for POS Terminals

The contents of the receipt must be in accordance with the following minimum requirements:

1. 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);
2. Transaction date;
3. Transaction type;
4. Account type selected (if supported);
5. primary account number (PAN)—(The PAN must be truncated as specified below);
6. POS Terminal number and/or location (retailer name and/or identification);
7. trace number;
8. Transaction time;
9. Transaction result; and
10. any other information required under applicable laws, Rules, and the regulations, policies, and technical specifications of the Corporation.

Refer to Rule 7.15.5 of this rulebook for the Transaction receipt requirements applicable to currency conversion by the Acquirer.

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 17, "Europe Region," of this rulebook.

7.15.2 Receipt Contents for Terminals

The contents of the receipt must be in accordance with the following minimum requirements:

1. identification of the Acquirer (*e.g.* institution name, logotype);
2. local time;
3. local date;
4. 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);
5. Terminal identification;
6. Card identification (PAN must be truncated as specified below)
7. Transaction type;
8. Transaction sequence number; and
9. a statement that the Transaction was for the purchase of goods or services (Merchandise Transaction only).

Refer to Rule 7.15.5 of this rulebook for the Transaction receipt requirements applicable to currency conversion by the Acquirer.

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 D, "Signage, Screen, and Receipt Text Standards."

7.15.3 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.

Refer to Rule 7.15.5 of this rulebook for the Transaction receipt requirements applicable to currency conversion by the Acquirer.

7.15.4 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.

7.15.5 Currency Conversion by the Acquirer or Merchant

If the Cardholder chooses currency conversion by the Acquirer or Merchant, then the receipt (or printable receipt page) must include all of the following information:

- The sales total amount in the currency in which goods or services are priced, or the amount of currency dispensed;
- The Transaction amount after conversion by the Acquirer or Merchant;
- The currency symbol or code of each;
- The method by which the currency agreed to by the Cardholder was converted from the sales total amount or from the amount of currency dispensed (for example, conversion rate); and
- Either of the following statements: "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" or "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."

7.15.6 PAN Truncation Requirements

7.15.6.1 POS Terminals

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

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

Solely with respect to any deployed POS Terminal currently producing Cardholder receipts that properly reflect only the last four (4) digits of the PAN, the POS Terminal software changes required to exclude the Card expiration date from the Cardholder receipt may be implemented with a future software update, but no later than 31 December 2010.

NOTE

A regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

7.15.6.2 Terminal

The Cardholder receipts generated by all Terminals must omit the Card expiration date. In addition, the Cardholder receipt generated by all Terminals must reflect only the last four (4) digits of the PAN. All preceding digits of the PAN must be replaced with fill characters that are neither blank spaces nor numeric characters, such as "x," "*", or "#".

Solely with respect to any deployed Terminal currently producing Cardholder receipts that properly reflect only the last four (4) digits of the PAN, the Terminal software changes required to exclude the Card expiration date from the Cardholder receipt may be implemented with a future software update, but no later than 31 December 2010.

NOTE

A regional Rule variation on this topic appears in Chapter 16, "Canada Region," of this rulebook.

7.15.7 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.

7.16 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 Connection to the Interchange System

Each Customer must connect to the Interchange System, and process all interregional Transactions via this system.

NOTE

An additional regional Rule on this topic appears in Chapter 16, "Canada Region," in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

7.17.1 ATM Connection to the Interchange System

Except as otherwise provided in the Rules, each Acquirer must at all times make available for connection to the Interchange System, all of the eligible ATMs established by that Acquirer (including its parents, subsidiaries, affiliates, and Sponsored entities) in the country where such Acquirer is located, and in every other country in which it has been Licensed to connect ATMs to the Interchange System.

Acquiring-only Customers must make available for connection to the Interchange System at least seventy-five percent (75%) of the online ATMs established by those entities.

NOTE

A regional Rule variation on this topic appears in Chapter 15, "Asia/Pacific Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

7.17.2 POS Terminal Connection to the Interchange System—Asia/Pacific Region and Latin America and the Caribbean Region Only

NOTE

Regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

7.17.3 Certification

Before beginning to process Transactions, a Principal must be certified in accordance with the Rules as qualified to interface with the Interchange System.

Periodically thereafter a Principal must certify, or be certified, with regard to such matters as required by the Corporation or the Rules. Failure to do so may result in the imposition of noncompliance assessment fees as provided in the Rules.

If a Customer, Service Provider, or Intermediate Network Facility (INF) makes a change to the software related to processing Transactions, the Corporation must be advised of that change. Based on that information, the Corporation will determine whether re-certification is appropriate.

For certification information, refer to the technical specifications.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region" and Chapter 20, "United States Region," of this rulebook.

7.17.4 Data Processing Facilities

A Principal has the right to connect at least one data processing facility directly to the Interchange System, or to a similar facility, which is owned or designated for such purpose by MasterCard.

A Principal must establish and maintain at their own expense a data processing facility that is capable of receiving, storing, processing, and communicating any Transaction sent to, or received from the Interchange System.

A Principal's data processing facility may be established and maintained by its parent, a wholly-owned subsidiary of such Principal, or any other affiliate of such Principal which is wholly owned, directly or indirectly, by the same parent as such Principal.

Alternatively, a Principal may designate a third party agent to establish and maintain its data processing facility provided that such agent is approved in advance by the Corporation and that such agent enters into an agreement with the Corporation, the form and substance of which have been approved by the Corporation.

7.17.5 Telecommunications

Customers must connect to the Interchange System via a telecommunications circuit established by the Interchange System equipped with backup service. All circuits must comply with the applicable technical specifications.

NOTE

An additional regional Rule on this topic appears in Chapter 20, "United States Region," of this rulebook.

7.17.6 Interface

Customers must develop and maintain the necessary computer hardware and software to interface with the Interchange System in accordance with the technical specifications and the Rules.

NOTE

An additional regional Rule on this topic appears in Chapter 20, "United States Region," of this rulebook.

7.17.7 Message Formats

Refer to the applicable technical specifications for message formats.

In cases where there are conflicts between the technical specifications and the Rules, the Rules will prevail.

NOTE

An additional regional Rule on this topic appears in Chapter 20, "United States Region," of this rulebook.

7.17.8 Testing

Processors must meet the minimum test requirements, as determined by the Corporation, before they begin production processing.

Test time will be assigned based on procedures outlined in the applicable technical specifications, and priorities defined by the Corporation.

Processors that have received initial approval to process Transactions must not stop production of Corporation processing to accomplish any periodic Interchange System testing, without prior permission of the Corporation.

The Customer Implementation department of MasterCard will arbitrate any disputes in the assignment of test time.

7.17.9 Customer Identification

Customers in the Corporation must identify themselves using a unique number, which is assigned by the Interchange System.

7.17.10 Routing Changes

Each Customer must notify the Corporation in writing of any routing updates, at least ten (10) business days before the effective date of the change. Expedited maintenance may be performed within two (2) business days of notice.

7.17.11 Hours of Operation

Customers must notify the Corporation of any scheduled downtime at least twenty-four (24) hours before such downtime.

NOTE

A regional Rule variation on this topic appears in Chapter 20, "United States Region," of this rulebook.

7.18 Card Capture

7.18.1 POS Transactions

Card capture is not supported for interregional POS Transactions.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook

7.18.2 ATM Transactions

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

Card capture at the ATM must only occur at the Issuer's direction. Cards captured as a result of the ATM's malfunction or Cardholder error (situations over which the ATM owner has no control) are the only allowable exceptions.

If the Acquirer cannot determine within two (2) business days if a Card was captured as a result of a machine malfunction or command sent by the Issuer, the Card will be deemed to be a Card captured on command of the Issuer.

7.18.2.1 Disposition of Command Captured Cards

Command captured Cards must have their magnetic stripe destroyed by the Acquirer. It is the responsibility of each Customer that captures a Card to establish the appropriate procedures within its own environment to ensure that Card capture is documented.

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

7.18.2.2 Disposition of Cards Captured Due to Machine Malfunction or Cardholder Error

Cards captured as a result of machine malfunction or Cardholder error should be maintained intact, and should be held at the ATM location, in a secure place, for two (2) business days following the day of capture.

Such captured Cards may be returned to the Cardholder in person, before the end of the second business day following the day of the Card capture, provided the Cardholder produces reasonable identification. Reasonable evidence of identity would include, for example, a current driver's license, passport, or similar identification with a picture or descriptive data and a signature that is comparable to the signature on the captured Card, if applicable.

In the event that the Card is returned to the Cardholder, a record of the action must be maintained by the Acquirer.

If the Cardholder does not return before the end of the second business day following Card capture to request the Card, the Card must have its magnetic stripe destroyed.

7.18.2.3 Disposition of Suspicious Captured Cards

Notwithstanding any of the requirements contained in Rule 7.18.2 of this rulebook, any Acquirer that captures a card that appears "suspicious" (for example, plain white plastic card, cardboard card or any other card that is unusual in nature) may at its option retain, preserve and release such card to appropriate law enforcement authorities.

7.18.2.4 Liability for Unauthorized Use

Acquirers will not incur liability for fraudulent or unauthorized Transactions initiated with a Card that such Acquirer has returned to a Cardholder following the Card's capture by an ATM, provided that such Acquirer acted in accordance with the provisions of this section of the Rules.

Acquirers will be liable for losses sustained by an Issuer for fraudulent or unauthorized Transactions which occur subsequent to Card capture, in all cases where such Acquirer allowed the use of the Card without complying with all portions of this chapter of the Rules.

7.18.2.5 Fee for Card Capture

The Acquirer must not charge the Issuer any fee for the capture and/or return of a Card or a MasterCard card.

7.19 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.

7.20 Merchandise Transactions

Merchandise may be any merchandise, service, or other thing of value within an Approved Merchandise Category, other than any merchandise, service, or other thing of value which:

1. is illegal or would tend to offend the public morality or sensibility, disparage the Corporation, or otherwise compromise the good will or name of the Corporation;
2. the Corporation has informed Acquirers, by way of private letter, bulletin, or other directive, are not permitted to be dispensed at ATMs; or
3. would permit the bearer thereof to obtain goods or services at a location other than an ATM, which, if dispensed at an ATM, would be prohibited pursuant to this section.

Promptly upon the Corporation's written direction, an Acquirer must cease dispensing at all its ATMs any Merchandise, which the Corporation has directed is not permitted.

ATMs dispensing Merchandise must also provide all other required Transactions as provided in Chapter 9, "Processing Requirements," of the Rules, and must conform to the screen display requirements in Chapter 7, "Acquiring," of the Rules.

Nothing in this section of the Rules or otherwise is deemed to authorize the display of the Marks, or initiation of a Transaction, at a Merchant location or any location other than an ATM fully conforming to the requirements of the Rules.

7.20.1 Approved Merchandise Categories

Approved Merchandise Categories are as follows.

Merchandise Category	Explanation
Postage Stamps	Stamps issued by the US Postal Service.
Event Tickets	Admission tickets to scheduled events that upon presentation of such tickets will admit the bearer to such scheduled events in lieu of other forms of admission tickets.
Transportation Tickets and Passes	Tickets or passes to board and ride scheduled transportation conveyances in lieu of other forms of transportation tickets.
Telecommunications Cards and Services	Prepaid telephone cards that entitle the holder to a specified amount of prepaid time or prepaid wireless telephone time that is credited to a subscriber's prepaid telephone account.

Merchandise Category	Explanation
Retail Mall Gift Certificates	Gift certificates to be sold at ATMs located in Retail Shopping Malls and redeemable for merchandise at stores located in the Mall where dispensed. Customers must receive prior written approval from the Corporation for each specific Mall implementation.
Charitable Donation Vouchers	Pre-valued donation vouchers that are dispensed as receipts for donations resulting from an authorized Transaction at a participating ATM. Customers must receive prior written approval from the Corporation for each specific charitable entity.

NOTE

A regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

7.20.2 Screen Display Requirements for Merchandise Transactions

The Acquirer must provide full disclosure to the Cardholder via the video monitor screen prior to the initiation of any Merchandise Transaction as detailed below. Disclosure must include the following:

1. full identification of the price and quantity of the Merchandise;
2. any additional shipping or handling charges (for mailed purchases only);
3. policy on refunds or returns; and
4. provision for recourse concerning Cardholder complaints or questions.

7.21 Chained Transactions

Acquirers that deploy ATMs that do not retain the Card internally until the Transaction(s) being performed is completed must require the Cardholder to re-enter the PIN for every additional financial Transaction performed. This requirement applies to card swipe readers, card dip readers, and similar devices where a card is not held within the device, and is removed prior to Transaction completion.

7.22 ATM Transaction Branding

If an Acquirer, which is not a MasterCard Customer, acquires an ATM transaction initiated by a MasterCard card that does not display the Mark(s) and sends it through the Interchange System, that transaction is deemed to be a Transaction and all Rules regarding Transactions will apply.

7.23 ATM Access Fees

For purposes of this Rule 7.23, a Transaction is any Transaction which is routed through the Interchange System.

Nothing contained in this section affects the right of an Issuer to determine what fees, if any, to charge its cardholders.

7.23.1 Domestic Transactions

Cardholders will not be assessed or be required to pay ATM Access Fees or other fee types imposed, or advised of, at an ATM, in connection with a domestic Transaction (that is, one that takes place at a Terminal located in the same country where the Card was issued).

NOTE

Regional Rule variations on this topic appear in Chapter 15, "Asia/Pacific Region," Chapter 16, "Canada Region," Chapter 17, "Europe Region,"Chapter 18, "Latin America and the Caribbean," and Chapter 20, "United States Region," of this rulebook.

7.23.2 Cross-border Transactions

Unless prohibited by local law or regulations Acquirers, upon complying with the ATM Access Fee certification requirements of the Rules, may assess an ATM Access Fee on a cross-border Transaction (that is, one that takes place at a Terminal located outside the country where the Card was issued), so long as the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory fashion.

7.23.2.1 Transaction Field Specifications

At the time of each disbursement Transaction on which an ATM Access Fee is imposed, the Acquirer of such Transaction must transmit, in the field specified by the *Single Message System Specifications* manual, the amount of the ATM Access Fee separately from the amount of the cash disbursed in connection with such Transaction.

7.23.2.2 Non-discrimination Regarding ATM Access Fees

An Acquirer must not charge an ATM Access Fee in connection with a Transaction that is greater than the amount of any ATM Access Fee charged by that Acquirer in connection with the transactions of any network accepted at that Terminal.

7.23.2.3 Notification of ATM Access Fee

An Acquirer that plans to add an ATM Access Fee must notify its Sponsoring Principal, in writing, of its intent to do so prior to the planned first imposition of such ATM Access Fee by the Acquirer.

The Principal must update the Location Administration Tool (LAT) regarding its or its Affiliates' imposition of ATM Access Fees.

7.23.2.4 Cancellation of Transaction

Any Acquirer that plans to add an ATM Access Fee must notify the Cardholder with a screen display that states the ATM Access Fee policy and provides the Cardholder with an option to cancel the requested Transaction.

7.23.2.5 Terminal Signage, Screen Display, and Transaction Record Requirements

Any Acquirer that plans to add an ATM Access Fee to a Transaction must submit a proposed Terminal, screen display, and receipt "copy" that meets the requirements of the Rules to its Sponsoring Principal in writing for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen, and Receipt Text Displays" in part 2 of this rulebook).

The Sponsoring Principal has the right to determine the acceptability of any new or changes to previously approved signage, screen display, and receipt copy. In cases of conflict between the Acquirer and its Sponsoring Principal, the Corporation has the sole right to determine the acceptability of any and all signage, screen display, and receipt copy.

7.23.2.5.1 Additional Requirements for Terminal Signage

An Acquirer that plans to add an ATM Access Fee to a Transaction may optionally display signage that is clearly visible to Cardholders on or near all Terminals at which ATM Access Fees apply.

The minimum requirement for ATM Access Fee signage text is wording that clearly states:

1. the name of the ATM Owner and Principal;
2. that the Transaction will be subject to an ATM Access Fee that will be deducted from the Cardholder's Account in addition to any Issuer fees;
3. the amount of, calculation method of, or Corporation-approved generic signage regarding the ATM Access Fee;
4. that the ATM Access Fee is assessed by the Acquirer instead of the Issuer;
5. that the ATM Access Fee is assessed on cross-border Transactions only.

The minimum requirements for Terminal signage (physical characteristics) are as follows:

1. the signage must bear the heading "Fee Notice";
2. the size of the Terminal signage must be a minimum of four (4) inches in height by four (4) inches in width;
3. the text must be clearly visible to all. It is recommended that the text be a minimum of fourteen (14) point type;
4. the heading must be clearly visible to all. It is recommended that the text be a minimum of eighteen (18) point type.

A model for Terminal signage regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.2.5.2 Additional Requirements for Terminal Screen Display

An Acquirer that plans to add an ATM Access Fee to a Transaction must present a screen display message that is clearly visible to Cardholders on all Terminals at which ATM Access Fees apply. If the Cardholder is given the option of choosing a preferred language in which to conduct the Transaction, the screen display message concerning ATM Access Fees must be presented to the Cardholder in that chosen language.

If an Acquirer displays the Corporation-approved generic ATM Access Fee signage, the Acquirer must include the amount or calculation method of the ATM Access Fee as part of the Terminal screen display.

A model for the Terminal screen display regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.2.5.3 Additional Requirements for Transaction Records

Any Acquirer that adds an ATM Access Fee to a Transaction must make available to the Cardholder on its Terminal receipt the ATM Access Fee information required by this Rule 7.21.2.5.3, in addition to any other information the Acquirer elects to or is required to provide.

The minimum requirements for the Terminal receipt are:

1. a statement of the amount disbursed to the Cardholder;
2. a statement of the ATM Access Fee amount with language clearly indicating it is a fee imposed by the Acquirer;
3. a separate statement of the combined amount of the ATM Access Fee and the disbursed amount, with language clearly indicating that this amount will be deducted from the Cardholder's Account.

A model for the Terminal receipt text regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.24 Return Merchandise Adjustments, Credits, and Other Specific Terms of a Transaction—Asia/Pacific Region Only

NOTE

Regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," of this rulebook.

7.25 Shared Deposits—United States Region Only

NOTE

Regional Rule variations on this topic appear in Chapter 20, "United States Region," of this rulebook.

7.26 Discounts or Other Benefits at POS Terminals—Latin America and the Caribbean Region Only

NOTE

Regional Rules on this topic appear in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

7.27 Identification of *PayPass* Transactions—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
7.1 Acquirer Obligations and Activities	A
7.1.14 Currency Conversion	B
7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only	A
7.3 Additional Acquirer Obligations and Activities for Terminals	A

Rule Number/Rule Title	Category
7.4 Acquiring Electronic Commerce Transactions	A
7.5 Acquiring Payment Transactions	A
7.8 Eligible POI Terminals	A
7.9 POS Terminal and Terminal Requirements	A
7.10 Hybrid POS Terminal and Hybrid Terminal Requirements	A
7.11 Additional Requirements for POS Terminals	A
7.12 Additional Requirements for ATMs	A
7.13 Additional Requirements for PIN-based In-Branch Terminals	A
7.14 POI Terminal Transaction Log	A
7.15 Requirements for Transaction Receipts	B
7.15.5 Currency Conversion by the Acquirer or Merchant	B
7.15.6 PAN Truncation Requirements	A
7.16 POS Terminal and Terminal Availability	A
7.17 Connection to the Interchange System	A
7.18 Card Capture	A
7.20 Merchandise Transactions	B
7.21 Chained Transactions	A
7.23 ATM Access Fees	B

Chapter 8 Security

This chapter contains information about security requirements.

8.1 Compliance

The Corporation may request compliance reports in the form of checklists and attestations, on-site security reviews, audits, or a combination of the aforementioned at any time.

Customers must comply with all current editions of the security-related requirements for each product or device, such as:

1. Compliance Assessment and Security Testing (CAST) Program for chip implementation and Mobile Payment Device issuance
2. PIN and Terminal Security—PIN Entry Devices (PEDs) and Encrypting PIN Pads (EPPs)

   PCI Approved PIN Entry Devices

   Payment Card Industry EPP Security Requirements

   Payment Card Industry POS PED Security Requirements
3. PIN and Terminal Security—PIN Security

   Payment Card Industry PIN Security Requirements
4. any other requirements published by the Corporation from time to time.

Issuers should also refer to the *Issuer PIN Security Guidelines*.

The above-referenced publications can be located on MasterCard Connect. Payment Card Industry publications are located online at www.pcisecuritystandards.org.

8.2 Terminal Compliance Requirements

Terminals that participate in Corporation Activities must be compliant with all of the requirements set forth in this Chapter 8, "Security," of the Rules. If a Terminal is not compliant with one or more of the requirements contained in this chapter, the Acquirer must immediately disconnect that Terminal from the Interchange System or face the imposition of noncompliance assessment fees, possible liability for any subsequent fraudulent Transactions that result from the noncompliant status of the Terminal, and/or termination of its License to participate in Corporation Activities.

8.3 Customer Compliance with Card Production Standards

A Customer engaged in Card production for itself or for other Customers, must comply at all times with all Standards applicable to any vendor approved by the Corporation, including but not limited to those set forth in this chapter and in the following documents:

- *Card Design Standards*
- *Logical Security Requirements for Card Personalization*
- *MasterCard Physical Security Standards for Plastic Card Vendors*
- *Security Guidelines for Instant Card Issuance and Instant Card Personalization*

Card production activities subject to compliance with these Standards include, by way of example and not limitation, the treatment and safeguarding of Cards, Card manufacture, printing, embossing, encoding, and mailing, as well as to any phase of the production and distribution of Cards or Account information.

The Customer must keep any media containing any Cardholder information, including, without limitation, names, addresses, phone numbers, and Account numbers, in an area limited to specially-designated personnel having access on a need-to-know basis

8.3.1 Card Vendor Certification Requirements

Issuers must:

1. order Cards from a vendor certified as provided in Rule 8.3.1.1; and
2. require that their Card vendors conform to the Standards set forth in the *MasterCard Physical Security Standards for Plastic Card Vendors*.

Issuers that manufacture their own Cards must be certified by the Corporation. The Corporation reserves the right to inspect the Issuer's Card manufacturing facilities during business hours.

8.3.1.1 MasterCard Global Vendor Certification Program

The Corporation certifies vendors for Card production services under the Global Vendor Certification Program. The Corporation applies the certification process when a vendor requests certification for any of the following services:

- Manufacturing, embossing, and encoding Cards
- Personalizing Cards
- Mailing Cards to Cardholders
- Embedding and personalizing chips
- Data preparation

The program includes two phases of certification, which the Corporation may undertake simultaneously:

- Assessment of the physical security of the vendor's site, and
- Assessment of the logical security of the vendor's data network environment, hardware, and software. All personalizers using an Internet connection or wireless LAN to transfer Issuer or Cardholder data must also undergo a network security scan as described in Rule 8.6 of the Site Data Protection Program.

The list of vendors that the Corporation has certified to provide Card production services, *Certified Vendors (for Card Production Services of Any MasterCard, Maestro, or Cirrus Branded Card)* is continually updated. From time to time, the Corporation distributes the current list, which supersedes all previously published lists, in a *Global Security Bulletin*.

8.3.1.2 Card Design and Production

Prior to production, one full color reproduction of the Card with the appropriate Marks must be submitted to the Licensing & Approvals department for approval. When approval is granted, the manufacturer must send two (2) sample Cards of the actual printed stock to the Licensing & Approvals department.

Only after written confirmation of the Card design approval, may the manufacturer manufacture and deliver the Cards to the Issuer. Subsequent deliveries of an unchanged Card design do not require separate approval.

8.4 PIN and Key Management Security Requirements

All Customers acquiring PIN transactions must comply with the security requirements for PIN and key management as specified in the *Payment Card Industry PIN Security Requirements*.

All Customers performing Issuer PIN processing must refer to the *Issuer PIN Policy and Guidelines* for all aspects of Issuer PIN management and PIN key management including PIN selection, transmission, storage, usage guidance, and PIN change.

8.4.1 PIN Verification

The Issuer is permitted to use the PIN verification algorithm of its preference.

Refer to "PIN Generation Verification" in the *Single Message System Specifications*, Chapter 6, "Encryption," for more information about PIN verification that the Single Message System performs directly for Maestro Issuers.

Refer to "PIN Verification" in the *Authorization System Manual*, Chapter 9, "Authorization Services Details," for more information about the MasterCard PIN verification service, in which Single Message System performs PIN verification on behalf of MasterCard issuers, and the two PIN verification methods (IBM 3624 and ABA) supported by the PIN verification service.

Issuers should refer to the *Issuer PIN Security Guidelines* for more information about Cardholder and Issuer PIN selection.

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

8.4.2 Stand-In Authorization—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

8.4.3 PIN Transmission between Customer Host Systems and the Interchange System

For detailed requirements about PIN key management and related services, including key change intervals and emergency keys, refer to the manuals listed below. These manuals are available on MasterCard Connect through the Publications product.

For Transaction authorization request message routed through…	Refer to…
Single Message System	*Single Message System Specifications*
MasterCard Key Management Center via the On-behalf Key Management (OBKM) Interface	*On-behalf Key Management (OBKM) Document Set*

8.5 PIN Entry Device

Use of a PIN is required for all Transactions to verify the Cardholder except under the circumstances outlined in Rule 6.4.3 Use of PIN or Signature of this rulebook.

The first digit entered into the PIN entry device (PED) must be the high-order digit (far left). The last digit to be entered must be the low-order digit (far right).

The PED must incorporate a "clear" key to enable the user to retract incorrect depressions and must have an "enter" key to indicate completion of PIN entry.

Acquirers must ensure that POS Terminals:

1. contain a PED that is compliant with the *Payment Card Industry PIN Security Requirements*; and

2. installed on or after 1 July 2005 including replacements and refurbished PEDs, contain a PED that is compliant with the Payment Card Industry POS PED Security Requirements and Evaluation Program.

Effective 1 July 2010, all PEDs that are part of a POS Terminal must be compliant with the Payment Card Industry POS PED Security Requirements and Evaluation Program or appear on the list of approved devices published by the Corporation.

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

Acquirers must ensure that Terminals:

1. contain a PIN pad that is compliant with the *Payment Card Industry Encrypting PIN Pad Security Requirements* manual; and
2. installed on or after 1 October 2005, including replacements and refurbished Terminals, contain an encrypting PIN pad (EPP) that is compliant with the Payment Card Industry Encrypting PIN Pad Program Security Requirements and Evaluation Program.

As a requirement for EPP testing under the Payment Card Industry EPP Security Requirements and Evaluation Program, the EPP vendor must complete the forms in the *Payment Card Industry Encrypting PIN Pad Security Requirements* manual along with the questionnaire contained in the *Payment Card Industry Encrypting PIN Pad Evaluation Vendor Questionnaire*. The vendor must submit all forms together with the proper paperwork, plus required EPP samples, to the evaluation laboratory.

Each secure cryptographic device must be uniquely identifiable at the interface with connected network zones up to the authorization system of the Issuer.

8.6 POS Terminal Communication Protocol

8.6.1 Account Protection Standards

PCI Security Standards are technical and operational requirements established by the Payment Card Industry Security Standards Council (PCI SSC) to protect Cardholder data. The Corporation requires that all Customers that store, process or transmit Cardholder data and agents that store, process or transmit Cardholder data on the Customer's behalf adhere to the most current Payment Card Industry PIN Transmission Security program (PCI PTS) and Payment Card Industry Data Security Standard (PCI DSS). Customers and their agents also must ensure that:

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

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

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

All wireless Point-of-sale (POS) Terminals and Internet/stand-alone IP-enabled POS Terminals must support the encryption of Transaction and Cardholder data between the POS Terminal and the Acquirer host system using Corporation-approved encryption algorithms.

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

- *Payment Card Industry Data Security Standard* available at www.pcisecuritystandards.org
- *POS Terminal Security Program—Derived Test Requirements*
- *POS Terminal Security Program—Program Manual*
- *POS Terminal Security Program—Security Requirements*
- *POS Terminal Security Program—Vendor Questionnaire*
- *Security Guidelines for Wireless Technologies*; and
- Any other related security documents that the Corporation may publish from time to time.

8.7 Component Authentication

All components actively participating in the system must authenticate each other by means of cryptographic procedures; either explicitly by a specific authentication protocol or implicitly by correct execution of a cryptographic service providing the possession of secret information, for example, the shared key or the log on ID.

A component actively participates in the Corporation if, due to its position in the Corporation, it can evaluate, modify or process security-related information.

8.8 Triple DES Standards

Cardholder PINs must be protected between the Point-of-Interaction and the Issuer host system during online PIN-based Transactions as follows:

1. All PIN POS Terminals must be Triple DES, double key length (hereafter referred to as "Triple DES") capable and deployed in compliance with the requirements set forth in Rule 8.5 of this rulebook. It is strongly recommended that all POS Terminals be "Triple Des" compliant.
2. All ATMs must be "Triple DES" compliant and deployed in compliance with the requirements set forth in Rule 8.5 of this rulebook.
3. All Customer and processor host systems must support "Triple DES."
4. All Transactions routed to the Interchange System must be "Triple DES."

8.9 Account Data Compromise Events

Definitions

As used in this Rule 8.9, the following terms shall have the meaning set forth below:

Account Data Compromise Event or ADC Event—an occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of Account data.

Agent—any entity that stores, processes or has access to Account data by virtue of its contractual or other relationship, direct or indirect, with a Customer. For the avoidance of doubt, Agents include, but are not limited to, Merchants, TPPs and DSEs (regardless of whether the TPP or DSE is registered with the Corporation).

Customer—this term appears in the Definitions chapter of this manual. For the avoidance of doubt, for purposes of this Rule 8.9, any entity that the Corporation licenses to issue a Card(s) and/or to acquire a Transaction(s) shall be deemed to be a Customer.

Potential Account Data Compromise Event or Potential ADC Event—an occurrence that could result, directly or indirectly, in the unauthorized access to or disclosure of Account data.

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

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

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

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

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

Any Customer that is uncertain with respect to rights and obligations relating to or arising in connection with the Account Data Protection Standards and Programs set forth in this Chapter 8 should request advice from MasterCard Fraud Investigations.

Notwithstanding the generality of the foregoing, the relationship of network, system, and environment configurations with other networks, systems, and environments will often vary, and each ADC Event and Potential ADC Event tends to have its own particular set of circumstances. The Corporation has the sole authority to interpret and enforce the Standards, including those set forth in this chapter. Consistent with the foregoing and pursuant to the definitions set forth in Rule 8.9 above, the Corporation may determine, as a threshold matter, whether a given set of circumstances constitutes a single ADC Event or multiple ADC Events. In this regard, and by way of example, where a Customer or Merchant connects to, utilizes, accesses, or participates in a common network, system, or environment with one or more other Customers, Merchants, Service Providers, or third parties, a breach of the common network, system, or environment that results, directly or indirectly, in the compromise of local networks, systems, or environments connected thereto may be deemed to constitute a single ADC Event.

8.9.2 Responsibilities in Connection with ADC Events and Potential ADC Events

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

Should a Customer, in the Corporation's judgment, fail to fully cooperate with the Corporation's investigation of an ADC Event or Potential ADC Event, the Corporation (i) may infer that information sought by the Corporation, but not obtained as a result of the failure to cooperate, would be unfavorable to that Customer and (ii) may act upon that adverse inference in the application of the Standards. By way of example and not limitation, a failure to cooperate can result from a failure to provide requested information; a failure to cooperate with the Corporation's investigation guidelines, procedures, practices and the like; or a failure to ensure that the Corporation has reasonably unfettered access to the forensic examiner.

A Customer may not, by refusing to cooperate with the Corporation's investigation, avoid a determination that there was an ADC Event. Should a Customer fail without good cause to comply with its obligations under this Rule 8.9 or to respond fully and in a timely fashion to a request for information to which the Corporation is entitled under this Rule 8.9, the Corporation may draw an adverse inference that information to which the Corporation is entitled, but that was not timely obtained as a result of the Customer's noncompliance, would have supported or, where appropriate, confirmed a determination that there was an ADC Event.

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

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

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

A Customer is deemed to be aware of an ADC Event or Potential ADC Event when the Customer or the Customer's Agent first becomes aware of an ADC Event or a Potential ADC Event under circumstances that include, but are not limited to, any of the following:

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

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

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

1. Immediately commence a thorough investigation into the ADC Event or Potential ADC Event.
2. Immediately, and no later than within twenty-four (24) hours, identify, contain and mitigate the ADC Event or Potential ADC Event, secure Account data and preserve all information, in all media, concerning the ADC Event or Potential ADC Event, including:

a. Preserve and safeguard all potential evidence pertinent to a forensic examination of an ADC Event or Potential ADC Event;

b. Isolate compromised systems and media from the network;

c. Preserve all Intrusion Detection Systems, Intrusion Prevention System logs, all firewall, Web, database and events logs;

d. Document all incident response actions; and

e. Refrain from restarting or rebooting any compromised or potentially compromised system or taking equivalent or other action that would have the effect of eliminating or destroying information that could potentially provide evidence of an ADC Event or Potential ADC Event.

3. Within twenty-four (24) hours, and on an ongoing basis thereafter, submit to the Corporation all known or suspected facts concerning the ADC Event or Potential ADC Event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the ADC Event or Potential ADC Event.

4. Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to the Corporation, in the required format, all Account numbers and expiration dates associated with Account data that were actually or potentially accessed or disclosed in connection with the ADC Event or Potential ADC Event, and any additional information requested by the Corporation. As used herein, the obligation to obtain and provide Account numbers to the Corporation applies to any Account number in the BIN range assigned by the Corporation. This obligation applies regardless of how or why such Account numbers were received, processed or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature- or PIN-based) proprietary, or any other kind of payment transaction, incentive or reward program.

5. Within seventy-two (72) hours, engage the services of a PCI Forensic Investigator to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration and effects of the ADC Event or Potential ADC Event. The PCI Forensic Investigator engaged to conduct the investigation must not have provided the last PCI compliance report concerning the system or environment to be examined. Prior to the commencement of such PCI Forensic Investigator's investigation, the Customer must notify the Corporation of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by the Corporation or, if such preliminary approval is not obtained, of a modified proposal acceptable to the Corporation. The Corporation and the responsible Customer(s) may agree that a PCI Forensic Investigator's investigation of, investigation findings, and recommendations concerning fewer than all of the Merchants within the scope of the ADC Event or Potential ADC Event will be deemed to be representative of and used for purposes of the application of the Standards as the investigation findings and recommendations by the PCI Forensic Investigator with respect to all of the Merchants within the scope of the ADC Event or Potential ADC Event.

6. Within two (2) business days from the date on which the QIRA was engaged, identify to the Corporation the engaged QIRA and confirm that such QIRA has commenced its investigation.
7. Within three (3) business days from the commencement of the forensic investigation, ensure that the QIRA submits to the Corporation a preliminary forensic report detailing all investigative findings to date.
8. Within twenty (20) business days from the commencement of the forensic investigation, provide to the Corporation a final forensic report detailing all findings, conclusions and recommendations of the QIRA, continue to address any outstanding exposure, and implement all recommendations until the ADC Event or Potential ADC Event is resolved to the satisfaction of the Corporation. In connection with the independent forensic investigation and preparation of the final forensic report, no Customer may engage in or enter into (or permit an Agent to engage in or enter into) any conduct, agreement or understanding that would impair the completeness, accuracy or objectivity of any aspect of the forensic investigation or final forensic report. The Customer shall not engage in any conduct (or permit an Agent to engage in any conduct) that could or would influence, or undermine the independence of, the QIRA or undermine the reliability or integrity of the forensic investigation or final forensic report. By way of example, and not limitation, a Customer must not itself, or permit any of its Agents to, take any action or fail to take any action that would have the effect of:

    a. precluding, prohibiting or inhibiting the QIRA from communicating directly with the Corporation;
    b. permitting a Customer or its Agent to substantively edit or otherwise alter the forensic report; or
    c. directing the QIRA to withhold information from the Corporation.

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

8.9.2.2 Ongoing Procedures for ADC Events and Potential ADC Events

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

1. Provide weekly written status reports containing current, accurate and updated information concerning the ADC Event or Potential ADC Event, the steps being taken to investigate and remediate same, and such other information as the Corporation may request.
2. Preserve all files, data and other information pertinent to the ADC Event or Potential ADC Event, and refrain from taking any actions (*e.g.*, rebooting)

that could result in the alteration or loss of any such files, forensic data sources, including firewall and event log files, or other information.

3. Respond fully and promptly, in a manner prescribed by the Corporation, to any questions or other requests (including follow-up requests) from the Corporation with regard to the ADC Event or Potential ADC Event and the steps being taken to investigate and remediate same.
4. Authorize and require the QIRA to respond fully, directly, and promptly to any written or oral questions or other requests from the Corporation, and to so respond in the manner prescribed by the Corporation, with regard to the ADC Event or Potential ADC Event, including the steps being taken to investigate and remediate same.
5. Consent to, and cooperate with, any effort by the Corporation to engage and direct a QIRA to perform an investigation and prepare a forensic report concerning the ADC Event or Potential ADC Event, in the event that the Customer fails to satisfy any of the foregoing responsibilities.
6. Ensure that the compromised entity develops a remediation action plan, including implementation and milestone dates related to findings, corrective measures and recommendations identified by the QIRA and set forth in the final forensic report.
7. Monitor and validate that the compromised entity has fully implemented the remediation action plan, recommendations and corrective measures.

8.9.3 Forensic Report

The responsible Customer (or its Agent) must ensure that the QIRA retain and safeguard all draft forensic report(s) pertaining to the ADC Event or Potential ADC Event and, upon request of the Corporation, immediately provide to the Corporation any such draft. The final forensic report required under Rule 8.9.2.1 must include the following, unless otherwise directed in writing by the Corporation:

1. A statement of the scope of the forensic investigation, including sources of evidence and information used by the QIRA.
2. A network diagram, including all systems and network components within the scope of the forensic investigation. As part of this analysis, all system hardware and software versions, including POS applications and versions of applications, and hardware used by the compromised entity within the past twelve months, must be identified.
3. A payment card transaction flow depicting all points of interaction associated with the transmission, processing and storage of Account data and network diagrams.
4. A written analysis explaining the method(s) used to breach the subject entity's network or environment as well as method(s) used to access and exfiltrate Account data.

5. A written analysis explaining how the security breach was contained and the steps (and relevant dates of the steps) taken to ensure that Account data is no longer at risk of compromise.
6. An explanation of investigative methodology as well as identification of forensic data sources used to determine final report findings.
7. A determination and characterization of Account data at risk of compromise, including number of Accounts and at risk data elements (magnetic stripe data—track 1 and track 2, Cardholder name, PAN, expiration date, CVC 2, PIN and PIN block).
8. The location and number of Accounts where restricted Account data (magnetic stripe, track 1 and track 2, Cardholder name, PAN, expiration date, CVC 2, PIN, or PIN block), whether encrypted or unencrypted, was or may have been stored by the entity that was the subject of the forensic investigation. This includes restricted Account data that was or may have been stored in unallocated disk space, backup media and malicious software output files.
9. A time frame for Transactions involving Accounts determined to be at risk of compromise. If Transaction date/time is not able to be determined, file-creation timestamps must be supplied.
10. A determination of whether a security breach that exposed payment card data to compromise occurred.
11. On a requirement-by-requirement basis, a conclusion as to whether, at the time the ADC Event or Potential ADC Event occurred, each applicable PCI Security Standards Council requirement was complied with. For the avoidance of doubt, as of the date of the publication of these Standards, the PCI Security Standards include Payment Card Industry Data Security Standards (PCI DSS), PIN Entry Device Security Requirements (PCI PED), and Payment Application Data Security Standards (PA-DSS).

The Corporation may require the Customer to cause a QIRA to conduct a PCI GAP analysis and include the result of that analysis in the final forensic report.

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

8.9.4 Corporation Determination of ADC Event or Potential ADC Event

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

1. A Customer or its Agent acknowledges or confirms the occurrence of an ADC Event or Potential ADC Event;
2. Any QIRA report; or
3. Any information determined by the Corporation to be sufficiently reliable at the time of receipt.

8.9.4.1 Assessments for PCI Violations in Connection with ADC Events

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

8.9.4.2 Potential Reduction of Financial Responsibility

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

1. Substantiation to the Corporation from a PCI SSC-approved Qualified Security Assessor (QSA) of the compromised entity's compliance with the Payment Card Industry Data Security Standard (PCI DSS) at the time of the ADC Event or Potential ADC Event.
2. Reporting that certifies any Merchant(s) associated with the ADC Event or Potential ADC Event as compliant with the PCI DSS and all applicable MasterCard Site Data Protection (SDP) Program requirements at the time of the ADC Event or Potential ADC Event in accordance with Rule 8.10.4 of this rulebook. Effective 1 July 2012, such reporting must also affirm that all third party-provided payment applications used by the Merchant(s) associated with the ADC Event or Potential ADC Event are compliant with the PCI DSS, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the PCI PA-DSS Program Guide, found at pcisecuritystandards.org.

3. Registration of any TPP(s) or DSE(s) associated with the ADC Event under the MasterCard Registration Program (MRP), in accordance with Rule 8.10.6 of this manual.
4. Notification of an ADC Event or Potential ADC Event to and in cooperation with the Corporation and, as appropriate, law enforcement authorities.
5. Verification that the forensics investigation was initiated within seventy-two (72) hours of the ADC Event or Potential ADC Event and completed as soon as practical.
6. Timely receipt by the Corporation of the unedited (by other than the forensic examiner) forensics examination findings.
7. Evidence that the ADC Event or Potential ADC Event was not foreseeable or preventable by commercially reasonable means and that, on a continuing basis, best security practices were applied.

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

As soon as practicable, the Corporation will contact the Customer's Security Contact, Principal Contact and Merchant Acquirer Contact as they are listed in the Member Information—Cirrus/Maestro tool on MasterCard Connect, notifying all impacted parties of the impending financial obligation.

It is the sole responsibility of each Customer, not the Corporation, to include current and complete information in the Member Information—Cirrus/Maestro tool on MasterCard Connect.

NOTE

An addition to this Rule appears in Chapter 17, "Europe Region," of this rulebook.

8.9.4.3 Investigation and Other Costs

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

8.9.5 Assessments for Noncompliance

If the Customer fails to comply with the procedures set forth in this Rule 8.9, the Corporation may impose an assessment of up to USD 25,000 per day for each day that the Customer is noncompliant.

When an Issuer becomes aware that Account data has been lost, stolen, misplaced, or the like, by any person (for example, a tape of Account data is lost during transit to a storage site), the Issuer must report the occurrence as described above. The Corporation will determine in its sole discretion whether it considers such act to be an Account data compromise event.

8.10 Site Data Protection Program

Refer to Rule 8.6 of this rulebook for requirements for use of wireless local area network (LAN) technology. In addition to these requirements set forth in this Rule 8.10, Customers, Merchants, and Service Providers must comply with the requirements set forth in Rule 8.6 of this rulebook.

The Site Data Protection (SDP) Program is a program designed to encourage Customers, Merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect against Card data compromises. SDP facilitates the identification and correction of vulnerabilities in security processes, procedures, and Web site configurations. For the purposes of the SDP Program, Service Providers in this section refer to TPPs and DSEs.

Acquirers must implement the SDP Program by ensuring that their Merchants and Service Providers are compliant with the *Payment Card Industry Data Security Standard* (PCI DSS) and that all applicable third party-provided payment applications used by their Merchants and Service Providers are compliant with the *Payment Card Industry Payment Application Data Security Standard* (PCI PA-DSS) in accordance with the implementation schedule defined in Rule 8.10.5.

The *Payment Card Industry Data Security Standard* is a component of SDP; the *Payment Card Industry Payment Application Data Security Standard* sets forth security Standards that the Corporation hopes will be adopted as industry standards across the payment brands.

The Corporation has sole discretion to interpret and enforce the SDP Program Rules.

8.10.1 Payment Card Industry Data Security Standard

The *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* establishes data security requirements. Compliance with the *Payment Card Industry Data Security Standard* is required for all Issuer, Acquirers, Merchants, Service Providers, and any other person or entity a Customer permits, directly or indirectly, to store, transmit, or process Card data. Validation of compliance is only required for those entities specified in the SDP Program implementation schedule in Rule 8.10.5 of this rulebook. Effective 1 July 2012, all Merchants and Service Providers that use third party-provided payment applications must only use payment applications that are compliant with the *Payment Card Industry Payment Application Data Security Standard,* as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide.*

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

8.10.2 Compliance Validation Tools

As defined in the implementation schedule in Rule 8.10.5 of this rulebook, Merchants and Service Providers must validate their compliance with the *Payment Card Industry Data Security Standard* by using the following tools:

1. Onsite Reviews: The onsite review evaluates a Merchant's or Service Provider's compliance with the *Payment Card Industry Data Security 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 an independent assessor recognized by the Corporation as acceptable. Service Providers must use an acceptable third party assessor as defined on the SDP program Web site at www.mastercard.com/sdp. Onsite reviews must be conducted in accordance with the *PCI Security Audit Procedures* document available at www.pcisecuritystandards.org.
2. The *Payment Card Industry (PCI) Self-Assessment Questionnaire*: The *PCI Self-Assessment Questionnaire* is available at www.pcisecuritystandards.org. To be compliant, each Level 2, 3, and 4 Merchant and each Level 3 Service Providers must generate acceptable ratings on an annual basis.
3. 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, 2, and 3 Merchants, and all Service Providers, as required by the implementation schedule, must conduct scans on a quarterly basis using a vendor listed on the PCI SSC Web site. To be compliant, scanning and risk remediation must be conducted in accordance with the guidelines contained in the *Payment Card Industry (PCI) Security Scanning Procedures* available at www.pcisecuritystandards.org.

8.10.3 Vendor Compliance Testing

As part of the SDP Program, the Corporation provides a vendor compliance testing process for vendors that provide network scanning services. Technical requirements for network scanning vendors are provided in the *PCI DSS Security Scanning Procedures* available at www.pcisecuritystandards.org. For more information, Acquirers should visit the SDP program Web site at www.mastercard.com/sdp.

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

8.10.4 Acquirer Compliance Requirements

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

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

   a. the name and primary address of the Merchant;

   b. the name and phone number of the primary contact for the Merchant;

   c. the Merchant identification number for each of the Merchants;

   d. the name of each Service Provider that stores Card data on the Merchant's behalf;

   e. the number of Transactions that the Acquirer processed from the Merchant during the previous 12-month period;

   f. the Merchant's level under the implementation schedule provided in Rule 8.10.5 of this rulebook;

   g. The Merchant's compliance status with its applicable compliance validation requirements; and

   h. The Merchant's anticipated compliance date **or** the date on which the Merchant last validated its compliance (the "Merchant Validation Anniversary Date").

2. Communicate the SDP Program requirements to each Level 1, Level 2, and Level 3 Merchant, and validate the Merchant's compliance with the *Payment Card Industry Data Security Standard* by reviewing its *PCI Self-Assessment Questionnaire* available at www.pcisecuritystandards.org and the Reports on Compliance that result from network security scans and onsite reviews of the Merchant, if applicable.

3. Communicate the SDP Program requirements to each Level 1 and Level 2 Service Provider, and ensure that Merchants only use compliant Service Providers.

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

1. The Merchant has, when appropriate, engaged and used the services of a data security firm(s) considered acceptable by the Corporation for onsite review, security scanning, or both.

2. Upon reviewing the Merchant's onsite review results, *Payment Card Industry Self-assessment Questionnaire*, or network scan reports, the Acquirer has determined that the Merchant is in compliance with the *Payment Card Industry Data Security Standard* requirements.

3. On an ongoing basis, the Acquirer will monitor the Merchant's compliance. If at any time the Acquirer finds the Merchant to be noncompliant, the

Acquirer must notify the Corporation's SDP Department in writing at sdp@mastercard.com.

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

- Merchant principal data
- The name of any TPP or DSE that performs Transaction processing services for the Merchant's Transactions
- Whether the Merchant stores Card data

When considering a Merchant that performs Data Storage, Acquirers should carefully survey each Merchant's data processing environment. Merchants that do not store Card information in a database file still may accept payment card information via a Web page and therefore store Card data temporarily in memory files. Merchants that do not perform Data Storage never process the data in any form but may use a DSE for this purpose, such as in the case of a Merchant that outsources its environment to a Web hosting company, or an online Merchant that redirects customers to a payment page hosted by a third party.

8.10.5 Implementation Schedule

All onsite reviews, network security scans, and self-assessments must be conducted according to the guidelines in Rule 8.10.2 of this rulebook. For purposes of the SDP Program, Service Providers in this section refer to TPPs and DSEs.

The Corporation has the right to audit compliance with the SDP Program requirements. Noncompliance on or after the required implementation date may result in the following assessments.

Failure of the following to comply with the SDP Program mandate…	May result in an assessment of…
Classification	**Violations per calendar year**
Level 1 and Level 2 Merchants	Up to USD 25,000 for the first violation Up to USD 50,000 for the second violation Up to USD 100,000 for the third violation Up to USD 200,00 for the fourth violation
Level 3 Merchants	Up to USD 10,000 for the first violation Up to USD 20,000 for the second violation Up to USD 40,000 for the third violation Up to USD 80,00 for the fourth violation
Level 1 and Level 2 Service Providers	Up to USD 25,000 for the first violation Up to USD 50,000 for the second violation Up to USD 100,000 for the third violation Up to USD 200,00 for the fourth violation

Noncompliance also may result in Merchant termination, deregistration of a TPP as a Service Provider, or termination of an Acquirer's License pursuant to Chapter 1 of this rulebook.

The Acquirer must provide compliance action plans and quarterly compliance status reports for each Level 1, Level 2, and Level 3 Merchant using the SDP Acquirer Submission and Compliance Status form, available at www.mastercard.com/sdp or by contacting the MasterCard Site Data Protection Department at sdp@mastercard.com.

Acquirers must complete the form(s) in their entirety and submit the form(s) via e-mail to sdp@mastercard.com on or before the last day of the quarter, as follows.

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

Late submission or failure to submit the required form(s) may result in an additional assessment to the Acquirer as described for Category A (Payment System Integrity) violation in Rule 3.1.2.1.1 of this rulebook.

8.10.5.1 Merchants

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

Effective 1 July 2012, all Level 1, 2, and 3 Merchants that use any third party-provided payment applications must validate that each payment application used is listed on the PCI Security Standards Council Web site at www.pcisecuritystandards.org as compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*.

1. Level 1 Merchants

   A Merchant that meets any one or more of the following criteria is deemed to be a Level 1 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

a. Any Merchant that has suffered a hack or an attack that resulted in a Card data compromise; and

b. Any Merchant having greater than six million total combined MasterCard transactions and Maestro Transactions annually; and

c. Any Merchant meeting the Level 1 criteria of Visa; and

d. Any Merchant that the Corporation, in its sole discretion, determines should meet the Level 1 Merchant requirements to minimize risk to the system.

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

a. An annual onsite assessment conducted by a PCI Security Standards Council (SSC) approved Qualified Security Assessor (QSA) or internal auditor and

b. Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV).Effective 30 June 2012, Level 1 Merchants that use internal auditors for compliance validation must ensure that primary internal auditor staff engaged in validating compliance with the *Payment Card Industry Data Security Standard* attend PCI SSC-offered Internal Security Assessor (ISA) Program and pass the associated PCI SSC accreditation examination annually in order to continue to use internal auditors.

2. Level 2 Merchants

Unless deemed to be a Level 1 Merchant, the following are deemed to be a Level 2 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*

a. Any Merchant having greater than one million but less than or equal to six million total combined MasterCard transactions and Maestro Transactions annually; and

b. Any Merchant meeting the Level 2 criteria of Visa.

To validate compliance, each Level 2 Merchant must successfully complete:

a. An annual self-assessment; and

b. Quarterly network scans conducted by a PCI SSC ASV

Effective 30 June 2012, each Level 2 Merchant must ensure that staff engaged in self-assessing the Merchant's compliance with the *Payment Card Industry Data Security Standard* attend PCI SSC-offered Internal Security Assessor (ISA) Program and pass the associated PCI SSC accreditation examination annually in order to continue the option of self-assessment for compliance validation. Level 2 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

3. Level 3 Merchants

Unless deemed to be a Level 1 or Level 2 Merchant, the following are deemed to be a Level 3 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

a. Any Merchant having greater than 20,000 total combined MasterCard and Maestro e-commerce Transactions annually but less than or equal to one million total combined MasterCard and Maestro e-commerce transactions annually; and

b. Any Merchant meeting the Level 3 criteria of Visa.

To validate compliance, Level 3 Merchants must successfully complete:

a. An annual self-assessment; and

b. Quarterly network scans conducted by a PCI SSC ASV.

4. Level 4 Merchants

Any Merchant not deemed to be a Level 1, Level 2 or Level 3 Merchant is deemed to be a Level 4 Merchant. Compliance with the *Payment Card Industry Data Security Standard* is required for Level 4 Merchants; however validation of compliance (and all other MasterCard SDP Program Acquirer requirements set forth in Rule 8.10) is optional. However, a validation of compliance is strongly recommended for Acquirers with respect to each Level 4 Merchant in order to reduce the risk of Card data compromise and for an Acquirer to potentially gain a partial waiver of related assessments.

To validate compliance with the *Payment Card Industry Data Security Standard*, Level 4 Merchants must successfully complete:

a. An annual self-assessment; and

b. Quarterly network scans conducted by a PCI SSC ASV.

If a Level 4 Merchant has validated its compliance with the *Payment Card Industry Data Security Standard* and effective 1 July 2012, the *Payment Card Industry Payment Application Data Security Standard* as described in this section, the Acquirer may, at its option, fulfill the reporting and requirements described in Rule 8.10.4 of this rulebook.

8.10.5.2 Service Providers

Effective 1 July 2012, all Service Providers that use any third party-provided payment applications must validate that each payment application used is listed on the PCI Security Standards Council Web site at www.pcisecuritystandards.org as compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*.

1. Level 1 Service Providers

A Level 1 Service Provider is any TPP (regardless of volume) and any DSE that stores, transmits, or processes more than 300,000 total combined MasterCard transactions and Maestro Transactions annually.

Each Level 1 Service Provider must validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

a. An annual onsite assessment by a PCI SSC approved QSA, and

b. Quarterly network scans conducted by a PCI SSC ASV.

2. Level 2 Service Providers

A Level 2 Service Provider is any DSE that is not deemed a Level 1 Service Provider and that store, transmits, or processes 300,000 or less total combined MasterCard transactions and Maestro Transactions annually.

Each Level 2 Service Provider must validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

a. An annual self-assessment, and

b. Quarterly network scans conducted by a PCI SSC ASV.

8.10.5.3 MasterCard PCI DSS Risk-based Approach

A qualifying Level 1 or Level 2 Merchant located outside of the U.S. Region may use the MasterCard PCI DSS Risk-based Approach, under which the Merchant:

1. Validates compliance with the first four of the six total milestones set forth in the *PCI DSS Prioritized Approach* as follows:

   a. A Level 1 Merchant must validate compliance through an onsite assessment conducted by a PCI SSC-approved QSA, or by conducting an onsite assessment using internal resources that have been trained and certified through the PCI SSC-offered ISA Program.

   b. A Level 2 Merchant must validate compliance using a Self-Assessment Questionnaire (SAQ) completed by internal resources that have been trained and certified through the PCI SSC-offered ISA Program. Alternatively, a Level 2 Merchant may validate PCI DSS compliance via an onsite assessment

2. Annually revalidates compliance with milestones one through four using an SAQ. The SAQ must be completed by internal staff trained and currently certified through the PCI SSC-offered ISA Program.

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

1. The Merchant must certify that it is not storing sensitive Card authentication data, as such is defined in the *PCI Data Security Standard*, and which includes, by way of example and not limitation, the full contents of a Card's magnetic stripe or the equivalent on a chip, CVC 2 data, and PIN or PIN block data.

2. The Merchant must fully segregate its Card-not-present Transaction environment from its face-to-face Transaction environment. A face-to-face Transaction occurs when the Card, the Cardholder, and the Merchant representative are all present at the time of the Transaction.

3. For a Merchant located in the Europe Region, at least 95 percent of its annual total count of Card-present MasterCard transactions and Maestro Transactions must occur at Hybrid POS Terminals.
4. For a Merchant located in the Asia/Pacific Region, Canada Region, Latin America and the Caribbean Region, or South Asia/Middle East/Africa Region, at least 75 percent of the Merchant's annual total count of Card-present MasterCard transactions and Maestro Transactions must occur at Hybrid POS Terminals.
5. The Merchant must not have experienced an ADC Event within the last twelve (12) months. At the Corporation's discretion, this and other criteria may be waived if the Merchant validated full PCI DSS compliance at the time of the ADC Event or Potential ADC Event.
6. The Merchant must establish and annually test an ADC Event incident response plan.

Information about the *PCI DSS Prioritized Approach* is available at: www.pcisecuritystandards.org/education/prioritized.shtml

8.10.5.4 PCI DSS Compliance Validation Exemption Program—U.S. Region Only

Effective 1 October 2012, a qualifying Level 1 or Level 2 Merchant located in the U.S. region may participate in the PCI DSS Compliance Validation Exemption Program (the "Exemption Program"), which exempts the Merchant from the requirement to annually validate its compliance with the PCI DSS.

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

1. The Merchant validated its compliance with the PCI DSS within the previous 12 months or, alternatively, has submitted to its Acquirer, and the Acquirer must have submitted to the Corporation, a defined remediation plan satisfactory to the Corporation designed to ensure that the Merchant achieves PCI DSS compliance based on a PCI DSS gap analysis;
2. The Merchant does not store sensitive Card authentication data, as such is defined in the PCI DSS, and which includes, by way of example and not limitation, the full contents of a Card's magnetic stripe or the equivalent on a chip, CVC 2 data, and PIN or PIN block data. The Acquirer must notify the Corporation through compliance validation reporting of the status of Merchant storage of sensitive Card authentication data;
3. The Merchant has not been identified by the Corporation as having experienced an ADC Event during the prior twelve (12) months.
4. The Merchant has established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements; and

5. At least 75 percent of the Merchant's annual total U.S.-acquired MasterCard Transaction and Maestro Transaction count is processed through Dual Interface Hybrid POS Terminals, as determined based on the Merchant's transactions processed during the previous twelve (12) months via the Global Clearing Management System and/or Single Message System. Transactions that were not processed by the Corporation may be included in the annual U.S.-acquired Transaction count if the data is readily available to the Corporation.

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

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

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

8.11 Algorithms

The choice of encipherment algorithm(s) is restricted to those approved in the applicable ISO standards. Refer to the "PIN and Key Management Security Requirements" of this chapter for further information.

8.11.1 Recording and Storing Clearing and Reconciliation Data

If a POS Terminal or Terminal has a removable storage medium and the data is not protected by encipherment, only the minimum data necessary for clearing and reconciliation must be stored.

Sensitive data elements residing in the discretionary data field in track 2 such as PVV and CVV must not be recorded in the clearing and reconciliation data.

8.12 Message Integrity

Customers must ensure that Transaction messages are protected against fraudulent modification. For additional information please refer to the *Message Integrity Guidelines* located on MasterCard Connect.

8.13 Signature-based Transactions—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

8.14 Audit Trail—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

8.15 Inspection of Customers—Europe Region Only

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
8.1 Compliance	A
8.2 Terminal Compliance Requirements	A
8.3.1 Card Vendor Certification Requirements	A
8.4 PIN and Key Management Security Requirements	A
8.5 PIN Entry Device	A
8.6 POS Terminal Communication Protocol	A
8.7 Component Authentication	A
8.8 Triple DES Standardss	A
8.9 Account Data Compromise Events	A
8.10 Site Data Protection Program	A
8.11 Algorithms	A
8.12 Message Integrity	A

Chapter 9 Processing Requirements

This chapter contains information about processing requirements.

9.1 Interchange Processing

MasterCard provides interregional processing of Transactions via the Single Message System.

9.2 POS Transaction Types

9.2.1 Issuer Online POS Transactions

All Issuers or their agents must ensure that system interfaces support the following online Transactions:

1. purchase from primary Account
2. purchase from checking Account
3. purchase from savings Account
4. pre-authorization from primary Account
5. pre-authorization from checking Account
6. pre-authorization from savings Account
7. refund
8. correction (appears as reversal)
9. reversal
10. Payment Transaction
11. Mobile Remote Payment

Effective in 2020 with Release 20.1, Issuers must support partial approval for all card account ranges and balance response for all prepaid Card account ranges.

Issuers that permit their Cardholders to perform electronic commerce Transactions must additionally support the Account in Good Standing, non-financial Transaction.

While Issuers or their agents' host computer system interfaces must support the online Transactions listed in this Rule 9.2.1, Issuers are not required to offer all of these Transaction types to their Cardholders. If an Issuer chooses not to offer one or more of the above-listed Transaction types to its Cardholders, the Issuer must send a message indicating that "transaction not permitted to issuer/cardholder" (in the Single Message System a response code 57) in the online authorization message.

NOTE

A regional Rule variation to the above rule appears in Chapter 17, "Europe Region," of this rulebook.

A refund Transaction may be processed without PIN verification. An Issuer must not decline authorization of a refund Transaction solely because no PIN was present in the authorization message. For Maestro *PayPass*, Issuers do not need to support the refund Transaction.

Issuers within a Region may be required to support the balance inquiry Transaction.

An Issuer must not decline authorization of a Transaction solely because the PIN was verified in an offline mode or because the Transaction occurred in a country where Customers have been granted a waiver by the Corporation permitting them to use a signature-based CVM instead of a PIN-based CVM. For additional information concerning such countries, refer to Chapter 6, "Issuing."

An Issuer receiving a Reversal Request/0400 or an Acquirer Reversal Advice/0420 message must release any hold placed on the Account for the amount specified within 60 minutes of matching the reversal message to the original authorization response message.

NOTE

"Scrip" and "Merchant-approved" Transactions are received by Issuers as "purchase" Transactions.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," and a regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

9.2.2 Acquirer Online POS Transactions

9.2.2.1 Required Transactions

Acquirers and Merchants must ensure that each POS Terminal supports the electronic processing of the following online POS Transactions:

1. 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 Corporation has given a waiver, a signature to identify the Cardholder except in the case of properly presented Maestro *PayPass* Transactions where no CVM is required. Refer to Chapter 7, "Acquiring," for additional "card reader" information.

2. 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.

3. Partial approval:

   Effective in 2020 with Release 20.1, Acquirers must support partial approval for Merchants identified with MCC 5542 (Fuel Dispenser, Automated), or with an MCC listed in the table below with respect to Transactions conducted at attended POS Terminals.

MCC	Description
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5612	Women's Ready to Wear Stores
5691	Men's and Women's Clothing Stores
5732	Electronic Sales
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5999	Miscellaneous and Specialty Retail Stores

4. Balance response

   Effective in 2020 with Release 20.1, Acquirers must support account balance response for Merchants identified with an MCC listed in the table below with respect to Transactions conducted with a prepaid Card at an attended POS Terminal.

MCC	Description
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5612	Women's Ready to Wear Stores
5691	Men's and Women's Clothing Stores
5732	Electronic Sales
5812	Eating Places, Restaurants
5814	Fast Food Restaurants

MCC	Description
5912	Drug Stores, Pharmacies
5999	Miscellaneous and Specialty Retail Stores

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

NOTE

A regional Rule variation on this topic appears in Chapter 15, "Asia/Pacific Region," Chapter 17, "Europe Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook.

9.2.2.2 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:

1. Balance inquiry:

   Acquirers must ensure that balance inquiries, if supported, are initiated using a PIN and a Card.

2. Purchase variations as follows:

   a. 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.

   b. 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 17, "Europe Region," Chapter 19, "South Asia/Middle East/Africa Region," and Chapter 20, "United States Region," of this rulebook.

c. Merchant-approved Transaction;

Merchant-approved Transactions may be processed by the Acquirer, providing specific written approval to process such Transactions has been given by the Corporation. The Acquirer must strictly adhere to the 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 are not required to assist Acquirers in any attempt to collect on Merchant-approved Transactions.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

d. Partial approval:

Effective 1 November 2008, Acquirers and Merchants may choose to support this Transaction type. Acquirers and Merchants that choose to provide the partial approval Transaction must establish an education program relating to split-tender Transactions for retail employee staff including, but not limited to, POS terminal operators.

e. 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.

f. 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.

g. Balance response.

Effective 1 November 2008, Acquirers and Merchants may choose to support this Transaction type.

h. Cancel.

i. Refund.

j. Payment Transaction and MasterCard *MoneySend* Payment Transaction:

Neither a Payment Transaction nor a MasterCard *MoneySend* Payment Transaction may be effected to reverse a prior POS Transaction. A MasterCard *MoneySend* Payment Transaction must not be sent to a MasterCard card issued in India that is linked to a credit account.

k. Mobile Remote Payment Transaction:

A Mobile Remote Payment Transaction must be initiated from a Cardholder's Mobile Device for Personal PIN Entry. Acquirers participating in a Mobile Remote Payments program must comply with the requirements document in the *Mobile Remote Payments Program Guide*.

l. Reversal

An Acquirer or Merchant may convert an approved authorization of a Card-Not-Present (CNP) Transaction believed, in good faith, by the Acquirer or Merchant to be fraudulent into a decline solely in accordance with the following procedure:

i. The Acquirer or Merchant must determine whether to proceed with a Transaction believed, in good faith, to be fraudulent within 72 hours of sending the original authorization request message.

ii. Upon deciding not to proceed with the Transaction and still within 72 hours of the original authorization request, the Acquirer or Merchant must:

1) Generate a reversal message that includes a reason code indicating that the Transaction was declined by the Acquirer or by the Merchant due to perceived fraud;

2) Disclose to the Cardholder that the Transaction cannot be completed at that time, and provide the Cardholder with valid customer service contact information (phone number or e-mail address) to respond to Cardholder calls or e-mail messages related to the cancelled order. The contact information should be that of the Acquirer, Merchant, or third party provider that made the decision not to proceed with the Transaction. Sharing the specific reason(s) for the decline is not recommended or required

The fraud potential of a Transaction typically is determined through fraud screening and fraud scoring services that involve the storage, transmission or processing of Card or Transaction data in compliance with the *Payment Card Industry Data Security Standard* (PCI DSS). The Acquirer must register any third party provider of such services as a Third Party Processor (TPP) as set forth in Rule 14.6.1 of this rulebook. The systematic decline by an Acquirer or Merchant of CNP Transactions arising from particular Cards, Issuers or geographic locations is a violation of Rule 7.1.8 (4) of this rulebook.

Each Acquirer that has an agreement with a Merchant to perform electronic commerce Transactions or Mobile Remote Payment Transaction must additionally support the Account in Good Standing, non-financial Transaction.

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

NOTE

A regional Rule variation on this topic appears in Chapter 15, "Asia/Pacific Region," and Chapter 20, "United States Region," of this rulebook.

9.2.3 Issuer Offline POS Transactions

All Chip Card Issuers or their agents who elect to process Chip Card Transactions offline must support the following offline Chip Card Transactions:

1. purchase
2. refund

While Issuers' or their agents' host computer system interfaces must support the offline Transactions listed in this Rule 9.2.3, Issuers are not required to offer all of these Transaction types to their Cardholders. If an Issuer chooses not to offer one or more of the above-listed Transaction types to its Cardholders, the Issuer must send the Transaction online for authorization or decline the Transaction offline.

An Issuer must accept a Transaction cleared online by an Acquirer after a completed offline Chip Card Transaction.

9.2.4 Acquirer Offline POS Transactions

Each Merchant and Acquirer may offer at each hybrid POS Terminal participating in the Corporation, offline processing of the following chip-read Transactions:

1. purchase
2. 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.

9.2.5 Offline Processing—POS Transactions

If a Transaction that may be processed offline cannot be so processed for any reason, 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 the Acquirer submits a Transaction into clearing that was fully authorized offline within five (5) calendar days of the Transaction date, the Acquirer will receive the benefit of an incentive interchange rate that is lower than the standard interchange rate for Transactions.

If the Acquirer submits a Transaction into clearing that was fully authorized offline after five (5) calendar days of the Transaction date, the Transaction is subject to the standard interchange rate.

If the Acquirer does not submit a Transaction into clearing that was fully authorized offline within seven (7) calendar days of the Transaction date, the Issuer may charge back that Transaction under certain circumstances. Refer to Chapter 11, "Exception Item Processing," for additional information.

9.3 Terminal Transaction Types

9.3.1 Issuer Requirements

Issuers must offer the following:

1. access to cash withdrawal, no Account specified
2. the purchase of Merchandise, from no Account specified

While Issuers or their agents' host computer system interfaces must support the online Transactions listed in this Rule 9.3.1, Issuers are not required to offer all of these Transaction types to their Cardholders. If an Issuer chooses not to offer one or more of the above-listed Transaction types to its Cardholders, the Issuer must send a message indicating that "transaction not permitted to issuer/cardholder" (in the Single Message System a response code 57) in the online authorization message.

NOTE

Additional regional Rules on this topic appear in Chapter 16, "Canada Region," Chapter 17, "Europe Region," and Chapter 20, "United States Region" of this rulebook.

9.3.1.1 Issuer—Optional Transactions

Issuers may offer their Cardholders access to the following Transactions, to the extent permitted by law and as permitted within a Region:

1. balance inquiries to checking and savings accounts;
2. transfer from checking account to savings account;
3. transfer from savings account to checking account.

NOTE

A regional Rule variation on this topic appears in Chapter 17, "Europe Region," and an additional regional Rule on this topic appears in Chapter 20, "United States Region" of this rulebook.

9.3.2 Acquirer Requirements

Terminals must offer cash withdrawals from an Account. (Refer to Chapter 6, "Issuing." Rule 6.1.3 of this rulebook 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 any other network accepted at that Terminal 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 16, "Canada Region," Chapter 17, "Europe Region," and Chapter 20, "United States Region" of this rulebook.

9.3.2.1 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 16, "Canada Region," and a Rule variation on this topic appears in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

9.3.3 Terminal Edit Specifications—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.4 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.

POS Special Transactions must not be effected using Maestro *PayPass*.

9.4.1 Processing Requirements—POS Unique Transaction Types

Cardholder entered PINs are required for the POS Transaction types outlined in this Rule 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:

1. Money Transfer—Merchant (MCC 4829)

   This MCC will be renamed Money Transfer effective with Release 12.Q4.

   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 location at which the money transfer is initiated. These Transactions include non–face-to-face Transactions, such as those facilitated through the Internet. 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. Customers 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.

2. Money Transfer—Member Financial Institution (MCC 6534)

   This MCC will be deleted effective with Release 12.Q4.

   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 Customer location at which the money transfer is initiated. Transactions include non–face-to-face Transactions, such as those facilitated through the Internet. Any fee charged and included in the total Transaction amount must be clearly disclosed to the Cardholder in advance of completing the Transaction.

3. Quasi Cash—Member Financial Institution (MCC 6050)

   A Transaction in which a Card is used to purchase travelers checks, foreign currency, money orders, precious metals, or savings bonds at a Customer financial institution. This MCC may also be used to identify Transactions in which a Customer financial institution accepts a Card in direct payment of an existing debt, such as a private label card or vehicle loan. MCC 6050 may not be used to identify any sale other than as described, including, by way of example and not limitation; gambling Transactions (MCC 7995 must be used); videotext Transactions (MCC 5967 must be used); the sale of any prescription drug (MCC 5122 or MCC 5912 must be used); or the sale of any tobacco product (MCC 5993 must be used). 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.

4. Quasi Cash—Merchant (MCC 6051)

   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 Customer financial institution. This MCC may also be used to identify a Transaction in which a Merchant accepts a Card for payment of an existing debt, such as a private label card or vehicle loan.

   MCC 6051 may not be used to identify any sale other than as described, including, by way of example and not limitation: gambling Transactions (MCC 7995 must be used); the sale of any prescription drug (MCC 5122 or MCC 5912 must be used); or the sale of any tobacco product (MCC 5993 must be used).

   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 Customer financial institution, use MCC 6010.

5. Gambling Transactions (MCC 7995)

   Any Transaction, other than an ATM or PIN-Based In-Branch Terminal Transaction, involving the placing of a wager, the purchase of a lottery ticket, in-flight commerce gaming, or the purchase of chips or other value usable for gambling in conjunction with gambling activities provided by wagering or betting establishments such as casinos, race tracks, jai alai frontons, card parlors, airline, and the like. 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.

Acquirers must identify all such gambling Transactions with MCC 7995 so that issuers are fully aware of the nature of these transactions. Acquirers must process face-to-face gambling Transactions in accordance with Rule 9.4.1. Acquirers must process remote gambling Transactions in accordance with Rule 9.4.2.

For other types of purchases associated with the establishment, such as food, lodging, or passage, use the MCC that best describes that Transaction.

6. Gambling—Horse Racing, Dog Racing (MCC 9754)

   Use of this MCC is restricted to Merchants located in the U.S. region that are properly registered with the Corporation as set forth in Chapter 20, Rule 7.4.1 in part 2 of this rulebook. The Acquirer may only use this MCC for Transactions resulting from gambling activity identified by the Acquirer as legal involving horse racing or dog racing.

7. Truck Stop Transactions (MCC 7511)

   This MCC will be deleted effective with Release 12.Q4.

   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.

9.4.2 Processing Requirements—Electronic Commerce Unique Transaction Types and Payment 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:

1. Payment Transaction—Customer Financial Institution (MCC 6532)
2. Payment Transaction—Merchant (MCC 6533)
3. MasterCard *MoneySend* Intracountry Payment Transaction (MCC 6536)

   NOTE

   Please see Chapter 17, "Europe Region Rules," Rule 7.6, "Acquiring MasterCard *MoneySend* Payment Transactions," for a regional rule variation.

4. MasterCard *MoneySend* Intercountry Payment Transaction (MCC 6537)

NOTE

A regional Rule on this topic appears in Chapter 19, "South Asia/Middle East/Africa Region," of this rulebook.

9.4.3 Processing Requirements—Transactions Performed on Board Planes, Trains, and Ships

NOTE

A regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

A Customer may process Transactions that arise from a hybrid POS Terminal that has no fixed location (for example, a POS Terminal aboard a plane, train, or ship) even if that POS Terminal does not have an online connection as long as:

1. The Cardholder is verified by the use of a PIN. As the environment will not permit an online PIN verification, only EMV POS Transactions will be possible in this environment.
2. The Transaction is used only by Merchants under the following MCCs:
   a. 5309 (Duty Free Stores);
   b. 4111 (Transportation—Suburban and Local Commuter Passenger, including Ferries); and
   c. 4112 (Passenger Railways)
3. The hybrid POS Terminal does not perform fallback procedures from chip to magnetic stripe.

   The Merchant will be authorized to process the Transaction offline under the Merchant-approved Transaction Rules set forth in Rule 9.2.2.2 (2.c). If the POS Terminal recommends against Transaction approval based on its own risk parameters, the Transaction must be declined.

9.4.4 Processing Requirements—Tollway Transactions

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.4.5 Processing Requirements—Parking Garage Transactions

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.4.6 Processing Requirements—Unattended Petrol POS Terminals

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.4.7 Processing Requirements—Mail Order/Telephone Order (MO/TO) Transactions (UK, Ireland, Turkey, and France)

NOTE

Additional regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.4.8 Gaming Payment Transactions—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.4.9 Processing Requirements—Recurring Payments

NOTE

Additional regional Rules and rule variations on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.5 Processing Requirements

Customers must submit to the Corporation, either directly or indirectly through their Sponsor, completed IRT and IDF input documents, no later than ten (10) business days prior to the requested effective date of live processing in the Corporation, which will be verified against the License Agreement on file prior to file update.

The Corporation may, at its discretion and upon request from a Principal, facilitate file updates of IRT and IDF input documents received less than ten (10) business days prior to the requested effective date of live processing in the Corporation. In these cases, the Principal will be subject to a forms handling fee for each IRT and IDF document processed.

The following requirements apply only to electronic functions performed by POI Terminals or Service Providers, and do not apply to manual functions performed at the POS:

1. Transactions initiated with a Card may not be declined due to BIN/IIN validation by POI Terminals or Service Providers.
2. Transactions initiated with a Card may not be declined by POI Terminals or Service Providers as a result of edits or validations performed on the following data elements:

    a. PAN length;

    b. expiration date;

    c. service code;

d. discretionary data; or

e. check digit.

Acquirers and TPPs are discouraged from editing the transposition check digit. See Appendix B, "Technical Specifications."

9.5.1 Track 1 Processing

Acquirers and TPPs must not perform tests or edits on track 1 for the purpose of disqualifying Cards from eligibility for processing within the Corporation.

9.5.2 PAN Processing

Acquirers and TPPs must accept all PAN lengths in Cards when such PAN lengths are in compliance with Chapter 6, "Issuing," of the Rules.

Acquirers and TPPs 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.

9.5.3 Card Data Processing

Acquirers and TPPs 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 TPPs 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 Manual*.

Acquirers and TPPs must accept all Card service code values, when such service code values are in compliance with Chapter 6, "Issuing," of the Rules.

Acquirers and TPPs 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.

9.5.4 Chip Card Processing

Acquirers must operate POS Terminals and Terminals that support chip technology 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 Corporation.

All Chip Card Transactions performed at hybrid POS Terminals which are over the floor limit defined by MasterCard must be authorized online to the Issuer, whether the magnetic stripe or chip is used to initiate the Transaction. Transactions performed at hybrid POS Terminals may not be authorized offline by means of the chip in the event that an online authorization cannot be completed for technical reasons.

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.

All hybrid POS Terminals and Terminals must perform fallback procedures, unless prohibited by the Corporation.

NOTE

For Europe region Rules about technical fallback at POS Terminals, ATMs, and PIN-Based In-Branch Terminals, refer respectively to Rules 7.11.1, 7.12.1. and 7.13.1 in Chapter 17, "Europe Region," of this rulebook.

9.6 Processing Mobile Remote Payment Transactions

Issuers that permit their Cardholders to perform Mobile Remote Payment Transactions must be capable of processing these Transactions when presented by an Acquirer.

Mobile Remote Payment Transactions must not be effected by Maestro *PayPass*. Acquirers must properly identify a Mobile Remote Payment Transaction. Refer to the *Mobile Remote Payments Program Guide* for additional information. All Mobile Remote Payment 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 Corporation.

The Merchant must accept and send unaltered, to the Interchange System, the thirteen (13) to nineteen (19)-digit PAN and the four (4) digits displayed in the expiration date field.

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.

9.6.1 Cardholder Verification Method (CVM) Policy for Mobile Remote Payment

Issuer Domain Mobile Remote Payment Transactions must use online PIN as the CVM. Alternatively, Issuers may choose to implement mobile specific credentials and a method of generating an Accountholder Authentication Value (AAV) as the CVM.

Acquirer Domain Mobile Remote Payment Transactions use mobile specific credentials generated by the Acquirer or its Service Manager as the Cardholder authentication method.

9.7 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.

Electronic commerce Transactions must not be effected by Maestro *PayPass*.

Acquirers must properly identify an electronic commerce Transaction.

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 Corporation.

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 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.

9.7.1 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.

9.8 Authorizations

9.8.1 Cash Withdrawal Transactions

Cash withdrawal Transactions must be either approved or denied for the amount requested. No "less than requested" authorizations will be permitted.

9.8.2 Transaction Routing

Each Customer must, in accordance with the Standards, ensure that each Cross-border Transaction (that is, one that takes place at a POS Terminal or Terminal located outside the country where the Card was issued) is processed through the Interchange System, unless one of the following conditions exist:

1. The Customer has applied for and received prior written approval from the Corporation to effect other arrangements;
2. The Customer has applied for and received certification from the Corporation with the network processing standards for any bilateral or multilateral arrangement entered into on or after 1 June 2009; or
3. Applicable law requires other arrangements, and only to the extent otherwise so required.

As used in this section, "processed" means authorized when required and cleared through the Interchange System.

If a cross-border transaction is not processed through the Interchange System and meets one of the conditions contained in Rule 9.8.2, 1 through 3 above, Customers shall also provide the Corporation with a report with respect to such cross-border transactions in a form as required by the Corporation on a time frame that is prescribed by the Corporation. Such report and all information contained therein shall be subject to Rule 3.7.2 of this rulebook.

NOTE

Additional regional Rules on this topic appear in Chapter 15, "Asia/Pacific Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook.

9.8.2.1 Existing Bilateral or Existing Multilateral Arrangements

In the event that any Customer is a party to a bilateral or multilateral arrangement established before 1 June 2009 and such Customer has not applied for and received prior written approval from the Corporation to effect such an arrangement, then such Customer must:

1. Register such bilateral or multilateral arrangement with the Corporation no later than 31 August 2009 and provide such other information as the Corporation may request in connection with an evaluation of the relevant arrangement against the network processing standards specified by the Corporation from time to time.
2. If such arrangement fails to meet or exceed such network processing standards, work with the Corporation in a good faith and timely manner to make such adjustments as may be required in order to achieve compliance.
3. In any event, Customers shall also provide the Corporation with a report with respect to such cross-border transactions in a form as required by the Corporation on a timeframe as prescribed by the Corporation. Such

report and all information contained therein shall be subject to Rule 3.7.2 of this rulebook.

NOTE

Additional regional Rules on this topic appear in Chapter 16, "Canada Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook. A regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

To initiate registration or application for certification, Customers must contact via e-mail: networkprocessingstandards@mastercard.com.

9.8.2.2 Ineligible Customers

A network, whose related marks are ineligible to appear on a Card pursuant to Rule 4.5 of this rulebook, shall be ineligible to enter into a Corporation-approved bilateral or multilateral arrangement pursuant to Rule 9.8.2 of this rulebook.

9.8.3 Default Routing

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.

9.8.4 Financial Institution Table Update

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. Once informed of a change, an Acquirer must confirm via an acknowledgment file that it has updated its host systems accordingly. Acquirers who do not default route to the Interchange System must use the FIT for routing before default routing to any competing network.

9.8.5 Chip Transaction Routing

Any Transaction generated by a MasterCard Application Identifier (AID) must be routed through the Interchange System, or as otherwise approved by the Corporation.

NOTE

Additional regional Rules and Rule variations on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.8.6 Location Information Requirements

9.8.6.1 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.

9.8.6.2 Terminal Location Reporting

Each Principal is required to provide the Corporation with current and accurate information regarding its and its Sponsored Affiliates' Terminals by updating quarterly the Location Administration Tool (LAT) located on MasterCard Connect.

9.8.7 Authorization Response Time

9.8.7.1 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 Rule 9.9 of the Rules for additional information regarding Stand-In Processing Service.

NOTE

Additional regional Rules on this topic appear in Chapter 20, "United States Region," of this rulebook. Regional rule variations on this topic appear in Chapter 17, "Europe Region," of this manual.

9.8.7.2 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 Corporation.

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 20, "United States Region," of this rulebook.

9.8.8 MasterCard *MoneySend* Payment Transaction Authorizations

MasterCard *MoneySend* Payment Transaction authorizations must be either approved or declined for the full Transaction amount. No partial approvals will be permitted.

An authorized MasterCard *MoneySend* Payment Transaction is irrevocable and should not be charged back. The Issuer may file a compliance case under limited circumstances. Refer to Chapter 12, Arbitration and Compliance, for additional information regarding a MasterCard *MoneySend* Payment Transaction compliance case.

The Acquirer may only reverse a MasterCard *MoneySend* Payment Transaction for reason of a documented clerical error. Any requests by the Acquirer to correct a clerical error will be approved or rejected at the discretion of the Issuer. The clerical error must be reversed within one (1) calendar day of the date that the MasterCard *MoneySend* Payment Transaction was authorized. 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.

9.8.9 Offline Chip Authorizations—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.8.10 Address Verification Service—Intracountry Transactions in UK Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.8.11 CVC 2 Mismatches—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.8.12 POS Terminal Transaction Routing—Canada Region Only

NOTE

Regional Rules on this topic appear in Chapter 16, "Canada Region," of this rulebook.

9.8.13 CVC 3 Verification—Latin America and the Caribbean Region Only

NOTE

A regional Rule on this topic appears in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

9.9 Performance Standards

Issuers and Acquirers that fail to meet performance standards may be subject to noncompliance assessments as set forth in Rule 9.9.3 below or may be mandated to implement the Stand-In Processing Service.

9.9.1 Issuer Standards

Issuer processors must maintain connectivity to the Interchange System twenty-four (24) hours a day, seven (7) days a week, to ensure global acceptance.

NOTE

Additional regional Rules and Rules variations on this topic appear in Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

9.9.1.1 Issuer Failure Rate (Substandard Level 1)

An Issuer failure rate that exceeds two percent (2%) for POS or ATM Transactions for two (2) consecutive months is substandard level 1 performance. The Issuer failure rate will not apply to a Processor until:

1. after the fourth calendar month of operation; or
2. upon processing five thousand (5,000) Transactions in a calendar month;

whichever occurs first.

Issuers that have been designated as having substandard level 1 performance may be subject to noncompliance assessments.

9.9.1.2 Issuer Failure Rate (Substandard Level 2)

An Issuer failure rate that exceeds three percent (3%) for POS or ATM Transactions for two (2) consecutive months is substandard level 2 performance. The Issuer failure rate will not apply to a Processor until:

1. after the fourth calendar month of operation; or
2. upon processing five thousand (5,000) Transactions in a calendar month;

whichever occurs first.

Issuers that have been designated as having substandard level 2 performance may be subject to noncompliance assessments and will be mandated to implement the Stand-In Processing Service.

9.9.1.3 Calculation of the Issuer Failure Rate

Dual Message System

The Issuer failure rate is calculated by taking the total number of Transactions declined due to Issuer unavailability, malfunction, or timeout dived by the total number of Transactions.

Single Message System

The Issuer failure rate is calculated according to the formula below:

The sum of the following ISO 8583 response codes:

1. 91—destination processor not available
2. 91s—destination processor not available
3. 96—system malfunction

Divided by the total POS or ATM Transactions processed through the Issuer connection to the Interchange System.

9.9.2 Acquirer Terminal Standards

9.9.2.1 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:

1. after the fourth calendar month of such Processor's operation; or
2. 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:

1. 13 invalid amount
2. 30 format error

Divided by the total number of POS and ATM Transactions processed through the Acquirer connection to the Interchange System.

9.9.3 Noncompliance Assessments for Substandard Performance

An Issuer or Acquirer that fails to meet the Corporation's performance standards may be subject to the following regional noncompliance assessments:

Occurrence	Penalty
First occurrence	USD 15,000
Second occurrence within the twelve (12)-month period following the first occurrence	USD 15,000
Third and any subsequent occurrence within the twelve (12)-month period following the second occurrence	USD 20,000

After completion of a full calendar year without any violations, a subsequent violation is counted as a first violation.

9.10 Currency Conversion Rates

When currency conversion is performed by the Corporation, the exchange rates will be determined by the Corporation. These exchange rates are updated daily.

9.11 Gateway Processing—ATM Transactions Only

9.11.1 Liability

The liability of the Corporation to Customers that use Gateway Processing for ATM Transaction processing errors is limited to actual damages up to the amount of the erroneous ATM Transaction(s).

9.11.2 Authorized Gateway Services

Only Gateway ATM Transactions for Gateway services formally authorized by MasterCard are allowed to use the Interchange System for routing and settlement of funds. Listed below are the currently authorized Gateway services:

1. PLUS System USA, Inc.
2. VISA USA, Inc.

9.11.3 Error Resolution

All Gateway Customers must refer disputes relating to the processing of Gateway ATM Transactions according to the rules that govern the individual ATM Transactions.

Error resolution is supported within Gateway Processing to the extent provided in the Rules, which govern the individual Transactions.

When a Gateway Customer uses the Corporation for Gateway Processing, error resolution requests must be processed in accordance with Chapter 11, "Exception Item Processing," of the Rules.

9.11.4 Technical Requirements for Gateway Processing

Processors that use Gateway Processing are subject to all response time, availability, and data transmission requirements defined in the Rules and the technical specifications of the Corporation.

9.12 Floor Limit Guidelines (POS Transactions)

The Corporation establishes floor limit values as a guideline for Customers to follow in their authorization process. The floor limit value is a maximum monetary amount above which the Merchant must obtain authorization before completing the chip Transaction.

9.12.1 Magnetic Stripe/Chip Applicability

Magnetic stripe Transactions must be authorized online.

Chip Transactions below or equal to the lesser of the offline limit established by the Issuer in the chip or the floor limit for POS Terminals defined in the *Quick Reference Booklet* may be authorized offline. Chip Transactions above the lower of these two limits must be authorized online.

9.12.2 Minimum Floor Limits

The Corporation establishes certain floor limits for POS Terminals to reduce the degree of risk associated with chip Transactions that are fully authorized offline. An Acquirer choosing to use a higher floor limit does so at its own risk in that an Issuer may treat a chip Transaction that was above the floor limit established by the Corporation as though it was subject to the floor limit established by the Corporation for all purposes, including, without limitation, charging back chip Transactions.

The minimum floor limits for POS Terminals defined in the *Quick Reference Booklet* apply to all chip Transactions.

An Acquirer may set POS Terminal floor limits applicable at the Merchant level for all chip Transactions. An Acquirer should not set a floor limit higher than the applicable minimum floor limit established by the Corporation as that floor limit will continue to apply between the Acquirer and the Issuer.

9.12.3 Equivalent Floor Limits

In some cases, floor limits stated in U.S. dollars cannot be expressed in a convenient number of units of other currencies. In cases where the U.S. dollar is not legal tender, the correct currency unit limit may be increased or reduced by an amount not to exceed 10% so that the floor limit can be expressed conveniently.

9.12.4 Floor Limit Changes

A Principal may request that the Corporation change the floor limits for its country, if the Customer sufficiently documents the reasons for the change. This documentation should include information about the reason for the change, competitive practices, average charge amounts, and other pertinent details, if the request is based on factors other than changes in currency exchange rates.

Send all requests for floor limit changes and the supporting documentation to:

Vice President of Security and Risk Services
MasterCard Worldwide
2000 Purchase Street
Purchase NY 10577-2509
USA

One or more of the following will review these requests: MasterCard staff, committees, and the Board. MasterCard will advise the Customer of any approved floor limit changes.

9.13 Ceiling Limit Guidelines (Maestro *PayPass* POS Transactions)

NOTE

A regional Rule variation and additional regional Rules on this topic appear in Chapter 17, "Europe Region," and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

The Corporation has established maximum Transaction amount ceiling limit values for the Maestro *PayPass* authorization process as detailed in the charts below. The Transaction amount ceiling limit value is a maximum monetary amount for which a Maestro *PayPass* Transaction may be effected.

A Principal may request that the Corporation change the ceiling limit value for the country in which it is located, if the Customer sufficiently documents the reasons for the change. This documentation should include information about the reason for the change, competitive practices, average charge amounts, and other pertinent details, if the request is based on factors other than changes in currency exchange rates. Upon approval by the Corporation, deviations from the maximum Transaction amount ceiling limit value will be published in this Rule 9.14 of the rulebook.

Maximum Transaction amount ceiling limit values for Maestro *PayPass* Transactions defined below apply to all Maestro *PayPass* Transactions that occur in the specified location.

For fraudulent Transactions that exceed the Transaction amount ceiling limit value, the Acquirer may be liable for chargebacks. Refer to Chapter 11, "Exception Item Processing" for additional information.

Asia/Pacific Region

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
American Samoa	50	USD
Australia	35	AUD
Brunei Darussalam	45	BND
Cambodia	50	USD
	200,000	KHR
China	100	CNY
Christmas Island	35	AUD
Cocos (Keeling) Islands	35	AUD
Cook Islands	35	NZD
Fiji	100	FJD

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
French Polynesia	5,000	XPF
Guam	50	USD
Heard and McDonald Islands	35	AUD
Hong Kong	500	HKD
Indonesia	125,000	IDR
Japan	2,500	JPY
Johnston Island	50	USD
Kiribati	35	AUD
Korea, Republic of	30,000	KRW
Lao People's Democratic Republic	50	USD
	40,000	LAK
Macau	500	MOP
Malaysia	150	MYR
Marshall Islands	50	USD
Micronesia	50	USD
Midway Islands	50	USD
Mongolia	60,000	MNT
Nauru	35	AUD
New Caledonia	5,000	XPF
New Zealand	35	NZD
Niue	35	NZD
Norfolk Island	35	AUD
Northern Mariana Islands	50	USD
Palau	50	USD
Papua New Guinea	100	PGK
Philippines	500	PHP
Pitcairn	35	NZD
Samoa	120	WST
Singapore	100	SGD
Solomon Islands	75,000	SBD

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Taiwan	3,000	TWD
Thailand	500	THB
Timor-Leste	50	USD
Tokelau	35	NZD
Tonga	80	TOP
Tuvalu	35	AUD
U.S. Minor Outlying Islands	50	USD
Vanuatu	5,000	VUV
	50	USD
Viet Nam	900,000	VND
Wake Island	50	USD
Wallis and Futuna	5,000	XPF

Canada Region

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Canada	50	CAD

Europe Region

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Albania	3,340	ALL
Andorra	25	EUR
Antarctica	200	NOK
Armenia	1,000	RUB
	12,100	AMD
Austria	25	EUR
Azerbaijan	25	AZN
Belarus	1,000	RUB
	95,950	BYR
Belgium	25	EUR
Bosnia and Herzegovina	50	BAM

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Bulgaria	50	BGN
Croatia	100	HRK
Cyprus	20	EUR
Czech Republic	500	CZK
Denmark	185	DKK
Estonia	300	EEK
Falkland Islands (Malvinas)	20	FKP
Faroe Islands	185	DKK
Finland	25	EUR
France	25	EUR
French Guiana	25	EUR
Georgia	20	GEL
Germany, Republic of	25	EUR
Gibraltar	20	GIP
Greece	25	EUR
Greenland	185	DKK
Guadeloupe	25	EUR
Holy See (Vatican City State)	25	EUR
Hungary	5,000	HUF
Iceland	4,200	ISK
Ireland	25	EUR
Israel	120	ILS
Italy	25	EUR
Kazakhstan	4,000	KZT
Kosovo, United Nations Mission in Kosovo (UNMIK)	25	EUR
Kyrgyzstan	1,000	RUB
	1,525	KGS
Latvia	15	LVL
Liechtenstein	40	CHF

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Lithuania	85	LTL
Luxembourg	25	EUR
Macedonia	1,530	MKD
Malta	25	EUR
Martinique	25	EUR
Moldova	390	MDL
Monaco	25	EUR
Montenegro	25	EUR
Netherlands	25	EUR
Norway	200	NOK
Poland	50	PLN
Portugal	20	EUR
Romania	100	RON
Russian Federation	1,000	RUB
San Marino	25	EUR
Serbia, Republic of	2,500	RSD
Slovak Republic	25	EUR
Slovenia	25	EUR
Spain	25	EUR
St Helena	20	SHP
St. Pierre and Miquelon	25	EUR
Svalbard and Jan Mayen	200	NOK
Sweden	235	SEK
Switzerland	40	CHF
Tajikistan	140	TJS
Turkey	35	TRY
Turkmenistan	1,000	RUB
	95	TMT
Ukraine	255	UAH

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
United Kingdom	20	GBP
Uzbekistan	52,500	UZS

Latin America and the Caribbean Region

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Anguilla	130	XCD
Antigua and Barbuda	65	XCD
Argentina	50	ARS
Aruba	90	AWG
Bahamas	25	BSD
Barbados	50	BBD
Belize	40	BZD
Bermuda	25	BMD
Bolivia, Plurinational State of	120	BOB
Brazil	50	BRL
Cayman Islands	40	KYD
Chile	12,000	CLP
Colombia	30,000	COP
Costa Rica	10	CRC
Dominica	130	XCD
Dominican Republic	865	DOP
Ecuador	15	USD
El Salvador	20	USD
Grenada	130	XCD
Guatemala	155	GTQ
Guyana	3,055	GYD
Haiti	945	HTG
Honduras	390	HNL
Jamaica	1,800	JMD
Mexico	250	MXN

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Montserrat	130	XCD
Netherlands Antilles	45	ANG
Nicaragua	385	NIO
Panama	20	PAB
	20	USD
Paraguay	72,000	PYG
Peru	45	PEN
Puerto Rico	25	USD
St. Kitts-Nevis	65	XCD
St. Lucia	130	XCD
St. Vincent and the Grenadines	130	XCD
Suriname	40	SRD
Trinidad and Tobago	155	TTD
Turks and Caicos Islands	25	USD
Uruguay	320	UYU
Venezuela, Bolivarian Republic of	65	VEF
Virgin Islands, British	25	USD
Virgin Islands, U.S.	25	USD

South Asia/Middle East/Africa Region

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Afghanistan	2,300	AFN
Algeria	3,630	DZD
Angola	4,615	AOA
Bahrain	20	BHD
Bangladesh	3,400	BDT
Benin	24,570	XOF
Bhutan	2,325	INR
	2,325	BTN
Botswana	335	BWP
Bouvet Island	300	NOK
British Indian Ocean Territory (BIOT)	50	USD
Burkina Faso	24,570	XOF
Burundi	60,400	BIF
Cameroon	24,570	XAF
Cape Verde	4,175	CVE
Central African Republic	24,570	XAF
Chad	24,570	XAF
Comoros	18,800	KMF
Congo	24,570	XAF
Côte D'Ivoire	24,570	XOF
Democratic Republic of the Congo	44,250	CDF
Djibouti	8,700	DJF
Egypt	75	EGP
Equatorial Guinea	24,570	XAF
Eritrea	670	ETB
Ethiopia	670	ETB
French Southern Territories	50	EUR

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Gabon	24,570	XAF
Gambia	1,325	GMD
Ghana	70	GHS
Guinea-Bissau	24,570	GWP
India	500	INR
Iraq	58,000	IQD
Jordan	35	JOD
Kenya	3,825	KES
Kuwait	5	KWD
Lebanon	30,000	LBP
Lesotho	350	LSL
Liberia	3,600	LRD
Libyan Arab Jamahiriya	50	USD
Madagascar	106,655	MGA
Malawi	7,490	MWK
Maldives	630	MVR
Mali	24,570	XOF
Mauritania	14,030	MRO
Mauritius	1,500	MUR
Morocco	420	MAD
Mozambique	1,675	MZN
Namibia	345	NAD
Nepal	3,635	NPR
Niger	24,570	XOF
Nigeria	7,370	NGN
Oman	20	OMR
Pakistan	4,230	PKR
Palestine	50	USD
Qatar	100	QAR

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
Reunion	50	EUR
Rwanda	28,875	RWF
Sao Tome and Principe	925,650	STD
Saudi Arabia	100	SAR
Senegal	24,570	XOF
Seychelles	550	SCR
Sierra Leone	192,750	SLL
Somalia	77,880	SOS
South Africa	100	ZAR
Sri Lanka	5,615	LKR
Swaziland	355	SZL
Syrian Arab Republic	2,280	SYP
Tanzania, United Republic of	74,715	TZS
Togo	24,570	XOF
Tunisia	70	TND
Uganda	109,400	UGX
United Arab Emirates	100	AED
Western Sahara	420	MAD
Yemen	11,775	YER
Zambia	238,960	ZMK

United States Region

Geographic Location	Ceiling Limit Amount	Ceiling Limit Currency
United States	50	USD

9.14 Euro Conversion—Timing

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

9.15 Clearing and Presentments—Europe Region Only

NOTE

A regional Rule variation on this topic appears in Chapter 17, "Europe Region," of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
9.2 POS Transaction Types	A
9.3 Terminal Transaction Types	A
9.4 Special Transaction Types	A
9.5 Processing Requirements	A
9.7 Processing Electronic Commerce Transactions	A
9.8 Authorizations	A
9.9 Performance Standards	A
9.10 Currency Conversion Rates	A
9.11 Gateway Processing—ATM Transactions Only	A
9.12 Floor Limit Guidelines (POS Transactions)	A
9.13 Ceiling Limit Guidelines (Maestro *PayPass* POS Transactions)	A

Chapter 10 Settlement and Reconciliation

This chapter contains information about settlement and reconciliation.

10.1 Definitions

As used in the Rules set forth in this Chapter 10, the following terms have the meanings set forth below:

- "Interchange fee" means an amount paid by the Acquirer to the Issuer with respect to the interchange of a POS or Merchandise Transaction. All references to interchange fees in this Chapter 10 mean both the levels of the fees and all qualifying criteria and conditions for their applicability.
- "Intracountry issuing Volume" means the issuing Volume resulting from Intracountry Transactions.
- "Intracountry acquiring Volume" means the acquiring Volume resulting from Intracountry Transactions.
- "Service fee" means an amount paid by the Issuer to the Acquirer with respect to the interchange of an ATM or PIN-Based In-Branch Terminal Transaction. All references to service fees in this Chapter 10 mean both the levels of the fees and all qualifying criteria and conditions for their applicability.

10.2 Settlement

The settlement process used by the Interchange System calculates each Customer's financial position regarding Transaction Activity, moves funds, and provides justification via reports and files. This information is provided every calendar day.

The net value of Transactions must be settled either:

1. via clearing through GCMS; or
2. via entries through the Automated Clearing House (ACH), submitted by the Single Message System on the next Interchange System Business Day after settlement.

Information regarding the Interchange System Business Day cut-off time may be found in the technical specifications of the Corporation.

If the Corporation does not support the local currency of a particular country in the regional settlement service, then each Customer engaged in Intracountry Transaction Activity in the country must participate in the Corporation's intracurrency settlement service for the country, if any.

NOTE

Additional regional Rules on this topic appear in Chapter 16, "Canada Region," Chapter 17, "Europe Region," and Chapter 20, "United States Region," of this rulebook.

10.2.1 Settlement Account

Each Principal must promptly settle their accounts with the Corporation and other Customers relating to Transactions, in accordance with the procedures set forth in the Rules, and the regulations, policies and technical specifications of the Corporation, as may be in effect from time to time.

10.2.2 Assessment for Late Settlement—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

10.2.3 Settlement Currency—United States Region Only

NOTE

Regional Rules on this topic appear in Chapter 20, "United States Region," of this rulebook.

10.2.4 Settlement Finality

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

10.3 Reconciliation

It is the responsibility of each Customer, directly or through its processor if any, to reconcile the totals and Transactions provided by the Interchange System, to its own internal records on a daily basis.

Any discrepancies, errors or adjustments must be reported to the Corporation within forty-eight (48) hours of discovery.

Refer to the applicable technical specifications for contact and further information.

NOTE

An additional regional Rule on this topic appears in Chapter 20, "United States Region," of this rulebook.

10.4 Failure of a Principal Customer to Discharge a Settlement Obligation

Subject to the limitation set forth in this Rule, if a Principal Customer fails to discharge a Settlement Obligation arising from or in connection with any Processed Transaction, the Corporation will satisfy such Settlement Obligation(s) to the extent such Settlement Obligation(s) is not otherwise satisfied.

To the extent the Corporation satisfies a Customer's Settlement Obligation, such satisfaction constitutes an automatic transfer, sale, and absolute assignment to the Corporation, and not an assignment for security purposes, of all right, title, and interest in the receivable. Such satisfaction of the Customer's Settlement Obligation also entitles the Corporation to all records and documents related to the receivable, including the name and address of each Cardholder or other person obligated to satisfy any part of the receivable. The Customer must promptly deliver all such records and documents to the Corporation or to the Corporation's designee. Any proceeds received by or on behalf of the Customer from any receivable must be held in trust by the Customer and paid to the Corporation as soon as practicable.

The Corporation may take any action the Corporation deems necessary or appropriate to protect its interest in the receivable and to protect the integrity of the affairs of the Corporation, such as, by way of example and not limitation, by:

1. Refusing or rejecting Transaction authorization requests relating to use of the Customer's Cards.
2. Establishing a settlement account for monies due to and from the Customer.
3. Without prior notice to the Customer, holding any monies due, directly or indirectly and for any purpose, to the Customer from the Corporation and any Settlement Obligation(s) due to the Customer and apply those monies to the amounts the Customer owes to the Corporation and to other Customers arising from Participation.
4. Listing some or all of a Customer's Card account numbers on the Electronic Warning Bulletin file, the international Warning Notice(s), or both, or in other or similar publications.
5. Effecting chargebacks on behalf of the Customer.
6. Overseeing the disposition of unused Card stock and any other media bearing security-sensitive information, including Card Account information.

The Corporation assumes no liability, responsibility, or obligation to satisfy, in full or in part:

1. A Settlement Obligation arising from or in connection with a Transaction that was not a Processed Transaction.
2. A Settlement Obligation arising from or in connection with a Transaction in which the Principal Customer, considered together with one or more of its Sponsored Affiliate Customers, acts as both the Issuer and the Acquirer.

3. A Settlement Obligation arising from or in connection with a Transaction in which the Issuer and Acquirer are related parties or are under common Control by one or more parents, holding companies, or other entities.
4. A Settlement Obligation arising from or in connection with any of the Principal Customer's Sponsored Affiliate Customer(s).

10.5 Collateral Collection through Settlement Accounts

In instances in which Customers are deemed to pose a risk of loss to the payment system and the Customer resists or excessively delays establishing a security agreement with the Corporation, the Corporation has the authority to collect the necessary collateral through such Customer's settlement accounts in addition to that Customer's other settlement obligations. This authority will be exercised only after a minimum of three (3) weeks from the time of the initial request for collateral or under circumstances in which the Corporation deems it essential to obtain collateral without further delay or jeopardy posed to the integrity of the settlement system. Customers will be given seven (7) calendar days notice of this collection and the term of this collection. (If collection will be made through GCMS, the IPM Fee Collection Code 1740 [Debit Collateral for Security Arrangement] will be used.)

NOTE

Customers in the Europe Region should also refer to Rule 13 in Chapter 17, "Europe Region," of this rulebook.

10.6 System Liquidity

If the Corporation requires funds to maintain System liquidity and to meet any obligations that a Customer or Customers have failed to discharge (for purposes of this section, "Non-discharged Customer Obligations"), the Corporation may collect funds directly from their settlement accounts of Customers upon reasonable notice to the Customers. In such event, the funds will be collected by the Corporation by:

1. Decreasing the gross daily settlement amounts of outgoing volumes of a Principal by up to five percent (5%) of the amount settled on one or more days; and
2. Increasing the gross daily settlement amounts of incoming volumes of Principals by up to five percent (5%) of the amount settled on one or more days.

This collection may continue as long as deemed necessary or appropriate to satisfy Non-discharged Customer Obligations and to ensure system liquidity or until the Corporation deems such collection no longer necessary or appropriate.

Collected funds are treated as advance payments on the sums that may be required from the Principal in the allocation among Customers of loss related to Non-discharged Customer Obligations. If the funds collected from a Customer exceed the amount ultimately allocated to it or in connection with a Non-discharged Customer Obligation, excess amount will be returned to the Customer with interest. If the funds collected from a Customer do not exceed the amount allocated to it, the Customer will pay any shortage to the Corporation with interest payments. Any interest payment by or to the Corporation will be based on the average effective Federal Reserve Fund's Earning Credit Rate (or if such rate is not published, a rate that the Corporation designates) during the time between the incidence of the Customer funding and the final allocation.

NOTE

Customers in the Europe Region should also refer to Rule 13 in Chapter 17, "Europe Region," of this rulebook.

10.7 Interchange and Service Fees

A Transaction settled between Customers gives rise to the payment of the appropriate interchange fee or service fee, as applicable. The Corporation has the right to establish default interchange fees and default service fees (hereafter referred to as "interchange fees," "service fees," or collectively, "fees"), it being understood that all such fees set by the Corporation apply only if there is no applicable bilateral interchange fee or service fee agreement between two Customers in place. The Corporation establishes all fees for Interregional Transactions and Intraregional Transactions, and may establish fees for Intracountry Transactions. The Corporation will inform Customers, as applicable, of all fees it establishes and may periodically publish fee tables. Unless an applicable bilateral interchange fee or service fee agreement between two Customers is in place, any intraregional or interregional fees established by the Corporation are binding on all Customers.

NOTE

An additional regional Rules on this topic appears in Chapter 17, "Europe Region" of this rulebook.

10.8 Establishment of Intracountry Interchange and Service Fees

This Rule 10.8 is applicable only to Intracountry Transactions.

If intracountry interchange and service fees are not established by the Corporation, such fees may be established in one of two ways: by agreement of Customers in the country as set forth in Rule 10.8.1 of this rulebook, or by application of intraregional interchange and service fees to Intracountry Transactions as set forth in Rule 10.8.2. Such fees may also be established by bilateral agreement between two Customers as set forth in Rule 10.8.3 of this rulebook.

For any Transaction that is subject to a bilateral agreement between two Customers, the interchange and service fees set forth in the bilateral agreement prevail.

For any Transaction that is not subject to a bilateral agreement between two Customers, the default intracountry fees established by the Corporation apply, or if none, the default intracountry fees established by Customers pursuant to these Rules apply, or if none, the intraregional fees apply, or if none, the interregional fees apply. Any multilateral Customer fee agreement must comply with all requirements set forth in Rule 10.8.1 of this rulebook. The Corporation reserves the right to determine if multiple bilateral agreements are deemed to be a multilateral agreement.

10.8.1 Default Intracountry Fees

If permitted by local law, default fees applicable to Intracountry Transactions for a country may be established by the affirmative vote of Customers that hold a License for the country and represent at least 75 percent of the intracountry issuing Volume (excluding on-us Volume) and at least 75 percent of the intracountry acquiring Volume (excluding on-us Volume) in the preceding calendar year. To be effective, and in addition to the foregoing, intracountry fallback fees must be agreed to by at least two Acquirers and at least two Issuers Licensed to engage in Activity in the country. Once effective, intracountry fallback fees remain in effect until revised by Customers pursuant to these Rules or by the Corporation.

Intracountry default fees established by Customers must be established with the purpose of encouraging the widespread use and acceptance of Cards, must be justifiable, must not jeopardize the integrity of the Interchange System, must not conflict with the Standards, and must be reviewed periodically (typically, every one to three years) and revised as appropriate.

Customers that establish intracountry default fees must promptly provide the Corporation with a copy of such fees and any subsequent change to the fees. Customers must be notified of intracountry default fees and any change thereto well in advance of the effective date, unless exceptional circumstances make this impossible. Exceptional circumstances generally must relate to events beyond the control of Customers; in the event of dispute or uncertainty, the Corporation determines if notice was effective. Intracountry default fees that have not been provided to and acknowledged by the Corporation as effective as of a certain date are not effective.

10.8.2 Intraregional Fees

In the event that no bilaterally agreed interchange fee or service fee applies and no default interchange fee or service fee has been otherwise established pursuant to these Rules, the applicable intraregional fee or if none, the interregional fee, applies to Intracountry Transactions.

10.8.3 Bilateral Agreement

Any two Customers may establish by bilateral agreement the interchange and service fees applicable to Transactions between them. All such fees must be submitted promptly to the Corporation. When applicable to Transactions processed through the Interchange System, they must be submitted to the Corporation sufficiently in advance of the effective date to allow the Corporation to incorporate the fees into future Interchange System releases as necessary or appropriate.

10.9 Cost Studies

The Corporation or its agent(s) may conduct one or more cost studies on a country-specific or regional or other basis for the purpose of establishing interchange and service fees. In order to ensure a sufficient quantity and level of data quality and representativeness as the Corporation deems necessary or appropriate, the Corporation may designate any number of Customers to participate in cost studies. All Customers so designated are required to participate and must provide and be able to certify that the Customer has provided the Corporation or its agent(s) with complete and accurate information in the form and manner and for such period of time and by a date as requested.

10.9.1 Allocation of Expenses

The Corporation may allocate expenses related to any cost study among Customers conducting Activity in the country or region or other area that is the subject of the cost study. The expenses may be allocated as the Corporation deems appropriate and the decision of the Corporation is binding on all Customers in that country or region or other area.

10.9.2 Noncompliance with a Cost Study

A Customer designated to participate in a cost study that fails to fully and timely participate is subject to assessments and other disciplinary action at the sole discretion of the Corporation.

10.10 Risk of Loss

Each Customer bears all risk of loss and the Corporation bears no risk of loss with respect to all amounts owed by the Customer under the Standards except to the extent any such amount is received by the Corporation, free and clear.

Each Customer remains fully responsible for fulfillment of, and must take all actions necessary to fulfill, all of its obligations under the Standards, regardless of whether the Customer designates a third party to perform all or any part of such obligations on the Customer's behalf. The fact that the Customer has paid any portion of the amounts owed to a third party does not discharge the Customer's obligations to the Corporation.

The Corporation may draw on the Customer's funds to fulfill any of the Customer's obligations under the Standards, regardless of whether those funds are held or controlled by the Customer or by any third party designee to the same extent the Corporation is entitled to draw on funds from any settlement account or funds of the Customer under the Standards, and regardless of whether those funds are commingled with any other funds. If the Corporation draws on the Customer's funds, the Corporation is not required to reimburse the Customer or any third party (whether a third party designee of the Customer or another Customer) for funds drawn which are owned by any of them or otherwise subject to any of their rights. The Customer and any third party (whether a third party designee of the Customer or another Customer) bear all risk and liability related to the funds drawn and must jointly and severally indemnify and hold the Corporation harmless from all liability and claims arising from any such draw of funds.

Each Customer bears all risk of loss and the Corporation bears no risk of loss with respect to all amounts owed by the Corporation to the Customer under the Standards once the payment is received by the Customer or any third party designee of the Customer, and regardless of whether or how such Transactions are cleared and settled using BINs not assigned to the Customer and/or settlement accounts not owned, controlled, possessed or maintained by the Customer.

Each Customer must notify the Corporation promptly in writing if the third party designee commingles funds received for or from the Customer in connection with the Customer's Transactions with any other funds.

Each Customer must notify the Corporation promptly in writing of the details of any failure of the Customer or any third party designee of the Customer to meet any of their obligations with respect to payment of funds owed under the Standards.

If a Customer's third party designee advances funds on behalf of the Customer to pay the Corporation or any other party entitled to receive those funds under the Standards, then such payment will be deemed to be a payment by the Customer, and the third party designee of the Customer, jointly and severally bear all risks of loss and hold the Corporation harmless from any all liability and claims arising from any such payment.

The Customer must:

1. obtain the written agreement of any third party designee of the Customer that may be given access to any funds owed by or to the Customer pursuant to the Standards; and
2. guarantee any such third party designee's compliance with all its obligations to the Corporation under this subsection of the Rules.

10.11 Customer Insolvency and Settlement Liability—Europe Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3, of the *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
10.2 Settlement	A
10.3 Reconciliation	A
10.5 Collateral Collection through Settlement Accounts	A
10.7 Interchange and Service Fees	A
10.8 Establishment of Intracountry Interchange and Service Fees	A
10.9 Cost Studies	A
10.10 Risk of Loss	A

Chapter 11 Exception Item Processing (REMOVED)

Content Relocated to Chargeback Guide.

Content Relocated to Chargeback Guide

The *Chargeback Guide* is the single source for all exception item processing and dispute resolution procedures. The rules that were formerly contained in this Chapter 11, "Exception Item Processing," have been incorporated into the *Chargeback Guide*.

Chapter 12 Arbitration and Compliance (REMOVED)

Content Relocated to Chargeback Guide.

Content Relocated to Chargeback Guide

The *Chargeback Guide* is the single source for all exception item processing and dispute resolution procedures. The rules that were formerly contained in this Chapter 12, "Arbitration and Compliance" have been incorporated into the *Chargeback Guide*.

Chapter 13 Liabilities and Indemnification

This chapter contains information about Customer and Corporation liabilities and indemnifications.

13.1 Warrant Compliance by Sponsored Customers

1. Every Principal warrants that each Customer it Sponsors will perform and discharge all its responsibilities, duties, obligations and liabilities arising in connection with the Rules, its License agreement, other applicable agreements, and the regulations, policies and technical specifications of the Corporation.

   Principals are liable to the Corporation and other Customers for the actions, or failures to act, of their Sponsored Customers to the same extent that such Principals would be liable if such actions, or failures to act, were their own.

2. All Customers make the same warranties and assume these same liabilities with regard to entities whose ATMs they connect, directly or indirectly, to the Interchange System, as they do with regard to Sponsored Customers, including, without limitation, those warranties and liabilities described in 13.1 (1) of this rulebook.

13.2 Liability of Affiliates

Each Affiliate is responsible for the liabilities and obligations arising out of, or in connection with, its Card programs or acquiring Activities which includes, but is not limited to, the obligation of a Customer to pay its Merchants, as required in Chapter 7, "Acquiring," Rule 7.2 (9) of this rulebook except to the extent any such liability or obligation has been previously satisfied by its Principal.

In accordance with the Standards and in compliance with applicable law, each Principal will have access to and may use or otherwise process its Sponsored Affiliates' confidential information and Confidential Transaction Data (as defined in Rule 3.7.2 of this rulebook) in connection with authorization, settlement, clearing, fraud reporting, chargebacks, billing, and other related activities.

13.3 Liability for Owned or Controlled Entities

For the purposes of this section, the term "customer" means a Customer (as such term is defined in the *MasterCard Rules* and Customer (as such term is defined in the *Maestro Global Rules* and the *Cirrus Worldwide Operating Rules*).

Each customer (a "Responsible Customer") shall irrevocably and unconditionally guarantee, as a primary obligor and not merely as a surety, to the Corporation and all other customers, the prompt payment and performance of the obligations (the "Guaranteed Obligations") of each of the Responsible Customer's affiliated entities arising under the Standards (as such term is defined in the *MasterCard Rules*, the *Maestro Global Rules*, and the *Cirrus Worldwide Operating Rules,* respectively), and from such affiliated entity's MasterCard, Maestro, and Cirrus Activities and use of the Marks (as defined in the *MasterCard Rules*) and the Marks (as such term is defined in the *Maestro Global Rules* and the *Cirrus Worldwide Operating Rules*).

For purposes of this section, a Responsible Customer's affiliated entity is defined as follows:

1. a Customer that is owned or Controlled by the Responsible Customer or is owned or Controlled by the Responsible Customer and another Customer or Customers;
2. a Customer that, with the Responsible Customer, is under common Ownership by or Control of another entity; or
3. a Customer that owns or Controls the Responsible Customer or shares Ownership or control of the Responsible Customer with another Customer or Customers.

The obligations of each Responsible Customer under this section shall be continuing, absolute, and unconditional and shall not be discharged or impaired or otherwise affected by any act or omission (including any renewal, extension, amendment, waiver or unenforceability of any of the Guaranteed Obligations) that may vary the risk of such Responsible Customer or otherwise operate as a discharge of the obligations of such Responsible Customer as a matter of law or equity, and all defenses of the Responsible Customer with respect thereto are waived to the fullest extent permitted by applicable law.

The Responsible Customer's liability to the Corporation and all other Customers is a primary obligation, while the Corporation's liability, if any, to another Customer is secondary, in that it only arises if a Responsible Customer is unable to pay its Guaranteed Obligations in full. Any assessments imposed on a customer for liability under this section may be collected by the Corporation, at its option, from the Customer's settlement account or by any other means available.

A Responsible Customer may not be exempted from the above-described liability except upon written notice by the General Counsel of the Corporation.

13.4 Limitation of Customer Liability

A Customer, solely by reason of its status as a Customer, is not personally responsible for any debts, liabilities, or obligations of the Corporation.

13.5 Limitation of Corporation Liability

The Corporation is not liable to any of its Customers or to any other entity that participates in the Corporation for any losses or damages that may arise in connection with participation in the Corporation.

13.6 Proprietary Card Mark

Each Issuer that uses a proprietary mark along with the Marks on its Cards assumes all responsibility and liability for use of the proprietary mark. Such Issuer must indemnify and hold harmless the Corporation and all other Customers, against any claim arising out of the Issuer's use of the proprietary mark, including but not limited to, claims of trademark or service mark infringement or dilution.

13.7 Stand-In Processed Transactions

Issuers will be liable for all Transactions authorized (with or without PIN validation) using the Stand-In Processing Service, provided that the Interchange System correctly uses the Stand-In Parameters defined by the Corporation, or the Issuer.

13.8 Pre-authorized Transactions

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 two (2) hours of the pre-authorization.

The Issuer's liability is limited to the amount of the pre-authorization, or the final Transaction, whichever is less.

NOTE

A regional rule variation on this topic appears in Chapter 15, "Asia/Pacific Region," and Chapter 20, "United States Region," of this rulebook.

13.9 Merchant-approved Transactions

An Issuer is not liable for any Merchant-approved Transaction, which is subsequently rejected by the Issuer upon electronic submission. However, if the Issuer accepts the Transaction on submission, or resubmission, the Issuer's liability is the same as for an online Transaction.

The Issuer must make reasonable efforts to collect the amount of such a rejected purchase Transaction, but in doing so, assumes no liability.

NOTE

Additional regional rules and a rule variation on this topic appear in Chapter 17, "Europe Region," of this rulebook.

13.10 Manually-entered PAN—Asia/Pacific Region and United States Region Only

NOTE

Regional rules on this topic appear in Chapter 15, "Asia/Pacific Region" and Chapter 20, "United States Region," of this rulebook.

13.11 Interchange System

13.11.1 Limitation of Liability

1. Except as provided under Rule 13.11.2 of this rulebook, the Corporation will have no responsibility or liability for any loss, cost, damage, claim, demand, cause of action, and expense, arising from any use or operation of the Interchange System, or failure to operate or use the Interchange System including, without limitation:

   a. the cost of investigating the claim;

   b. the cost of litigation and attorneys' fees; or

   c. any compensatory, punitive, special, incidental or consequential damages, including loss of profits

2. Additionally, the Corporation will have no liability for any failure of the Interchange System to operate or perform any function due to the following reasons, without limitation;

   a. downtime;

   b. natural disaster, fire, strike, riot, act of God or other causes, whether or not such causes are or may be within the Corporation's reasonable control or;

   c. any law, regulation, judicial decision or formal or informal administrative determination restricting or adversely affecting the ability of the Corporation to operate the Interchange System in accordance with the Rules. In this case, while the Corporation may cease operation, it will cooperate in good faith to continue its operations by making those modifications as may be reasonably required to comply with such law, regulation, decision, or determination.

13.11.2 Exceptions to Limitation of Liability

The Corporation will indemnify and hold harmless each Customer, against any liability, loss, cost, damage, claim, and expense, (including reasonable attorney's fees), that is directly attributable to the willful misconduct, intentional tort, fraud, or gross negligence of the Corporation, its agents, or its employees.

Each Customer must indemnify and hold harmless the Corporation against any other liability.

13.12 Indemnity and Limitation of Liability

Each Customer (for the purposes of this section an "Indemnifying Customer") must protect, indemnify, and hold harmless the Corporation and the Corporation's parent, subsidiaries, and affiliated entities, and each of the directors, officers, employees and agents of the Corporation and the Corporation's parent, subsidiaries, and affiliated entities from any actual or threatened claim, demand, obligation, loss, cost, liability and/or expense (including, without limitation, actual attorneys' fees, costs of investigation, and disbursements) resulting from and/or arising in connection with, any act or omission of the Indemnifying Customer, its subsidiaries, or any person associated with the Indemnifying Customer or its subsidiaries (including, without limitation, such Indemnifying Customer's directors, officers, employees and agents, all direct and indirect parents, subsidiaries, and affiliates of the Indemnifying Customer, the Indemnifying Customer's customers in connection with issuing and/or acquiring Activity and/or other business, and the Indemnifying Customer's suppliers, including, without limitation, any processors, Service Providers, and other persons acting for, or in connection with the Indemnifying Customer or a Merchant for which the Indemnifying Customer acquires Transactions, or any such Merchant's employees, representatives, agents suppliers, customers, including any Data Storage Entity (DSE) with respect to, or relating to:

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

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

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

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

NOTE

Additional regional rules on this topic appear in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

13.13 Additional Liabilities—Europe Region, Latin America and the Caribbean Region, and United States Region Only

NOTE

Regional Rules on this topic appear in Chapter 17, "Europe Region," Chapter 18, "Latin America and the Caribbean Region," and Chapter 20, "United States Region," of this rulebook.

13.14 Issuer Assurance Plan

NOTE

A regional Rule on this topic appears in Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

13.14.1 Program Participation

A Region may optionally participate in a program to indemnify their Issuers against actual fraud loss suffered from signature-based Transactions. Funds will be maintained in an account and administered by the Corporation.

Reimbursement for actual fraud loss may be claimed by the Region on behalf of the Issuer provided that:

1. the Region participates in the indemnification program;
2. other than PIN verification, the Issuer seeking indemnification used the applicable standard authorization procedures, (including verification that funds exist on account);
3. the Issuer seeking indemnification authorized the Transactions only after verifying that the components of the magnetic stripe data transmitted as part of the transaction request were consistent with Corporation encoding standards;
4. authorization was not given as a result of, or in connection with, the failure or malfunction of any system of the Issuer seeking indemnification, or the negligence or fraud of such Issuer or its Agents or personnel;
5. the Issuer seeking indemnification had not received notice or actual knowledge of loss, theft, or fraudulent use of the Card used in the Transaction, prior to authorizing the Transaction;
6. the Issuer seeking indemnification has obtained from the Cardholder a signed declaration that neither the Cardholder, nor any person authorized by the Cardholder, entered into the subject Transaction(s);
7. any other conditions as established by the Corporation are met.

13.14.2 Indemnification for Losses

Indemnification for losses associated with any one (1) PAN will not be provided beyond the following limits:

1. USD 1,000 per Transaction
2. USD 2,000 per day
3. USD 5,000 total

The indemnity covers only actual monetary loss, and not special, incidental or consequential damages.

The indemnity does not cover losses incurred on a Card also displaying the MasterCard mark unless the Card is used at a POI Terminal that does not accept MasterCard cards.

These limits do not prohibit any Issuer from authorizing Transactions and amounts outside the scope of the indemnity provided.

13.15 Disclaimer of Warranties

Neither Maestro, the Corporation, nor their affiliates makes any warranties whatsoever, expressed or implied, to any Customer or any other entity with regard to the services of the Corporation or with respect to the Marks or any other trademarks, tradenames, service marks, logotypes or trade designation of the Corporation, or with regard to any other matter whatsoever.

13.16 Enforceability of Rights

The Corporation may delay enforcing its rights under these Rules or forego the exercise of those rights, without losing or waiving any of such rights, either in the subject circumstances or any similar circumstances in the future.

13.17 Voidness

If any provision of the Rules is void or unenforceable in any jurisdiction, such voidness or unenforceability will not affect the validity or enforceability of any other provision of the Rules in that, or in any other jurisdiction.

13.18 Liability of Affiliates—Asia/Pacific Region Only

NOTE

A regional Rule on this topic appears in Chapter 15, "Asia/Pacific Region," of this rulebook.

Chapter 14 Service Providers

This chapter contains Rules that apply to Customers that use Service Providers to perform Program Service.

14.1 Service Provider Categories

As of the date of this publication of the Standards, there are four categories of Service Providers: Independent Sales Organization ("ISO"), Third Party Processor ("TPP"), Data Storage Entity ("DSE"), and Service Provider Registration Facilitator ("SPRF").

A Service Provider is categorized by the Corporation based upon the Corporation's understanding of the nature of the Program Service(s) performed or to be performed, as described below. A Service Provider may only perform the Program Service(s) it is registered to perform.

Any person proposed by a Customer to perform both TPP Program Service and DSE Program Service is categorized by the Corporation as a TPP.

A person that performs any one or more of the following Program Service…	Is categorized as this type of Service Provider:
ISO Program Service: • Merchant and/or Cardholder Solicitation, including application processing • Cardholder and/or Merchant customer service not involving access to Card data, Transaction data, or both, including the collection of any fee or other obligation associated with the Customer's Program • Merchant education and training • ATM deployment • any other service determined by the Corporation in its sole discretion to be ISO Program Service	Independent Sales Organization (ISO)
TPP Program Service: • Terminal operation with electronic data capture • authorization services, including but not limited to authorization routing, gateway and switching services, voice authorization, and call referral processing • clearing file preparation and submission • settlement processing (excluding possession, ownership, or control	Third Party Processor (TPP)

A person that performs any one or more of the following Program Service…	Is categorized as this type of Service Provider:
of settlement funds, which is not permitted) • Cardholder and/or Merchant statement preparation • Cardholder and/or Merchant customer service involving access to Card data, Transaction data, or both • fraud control and risk monitoring, including but not limited to fraud screening and fraud scoring services • chargeback processing • Mobile Remote Payment • any other service determined by the Corporation in its sole discretion to be TPP Program Service	
DSE Program Service: • Merchant Website hosting services • external hosting of payment applications, such as Web site shopping carts • Terminal driving and encryption key loading • any other service involving the storage, transmission or processing of Card data, Transaction data or both not identified by the Corporation as TPP Program Service	Data Storage Entity (DSE)
SPRF Program Service • identification of persons the Standards obligate a Customer to register as a Service Provider • assisting a Customer to register Service Providers other than SPRFs	Service Provider Registration Facilitator (SPRF)

14.1.1 Independent Sales Organization

An Independent Sales Organization ("ISO") is a Service Provider that performs any one or more of the services described in Rule 14.1 of this rulebook as ISO Program Service.

14.1.2 Third Party Processor

A Third Party Processor ("TPP") is a Service Provider that performs any one or more of the services described in Rule 14.1 of this rulebook as TPP Program Service.

TPPs are subcategorized as follows.

14.1.2.1 Type I

The first TPP subcategory is a Type I TPP. The Corporation determines, in its sole discretion, if a TPP is a Type I TPP. Type I TPPs generally are those that perform Program Service for a large number of Customers or that otherwise could significantly impact the integrity of the Interchange System.

As a condition of continued Type I TPP registration by the Corporation, a Type I TPP must comply with the Corporation's Type I TPP Evaluation Program requirements and applicable Standards, including these Service Provider Rules.

14.1.2.2 Type II

The second TPP subcategory is a Type II TPP. A Type II TPP is any TPP that the Corporation does not deem to be a Type I TPP. A Type II TPP must comply with applicable Standards, including these Service Provider Rules. The Corporation at any time may reclassify a Type II TPP as a Type I TPP.

14.1.3 Data Storage Entity

A Data Storage Entity ("DSE") is a Service Provider that performs any one or more of the services described in Rule 14.1 of this rulebook as DSE Program Service.

14.1.4 Service Provider Registration Facilitator

A Service Provider Registration Facilitator ("SPRF") is a Service Provider that performs Service Provider registration services, which is deemed by the Corporation to be a Program Service.

14.2 Determination of Program Service

Before a person commences to perform Program Service that directly or indirectly supports or otherwise benefits a Customer's Program(s), the Customer must cause such person to be registered by the Corporation as a Service Provider.

A Service Provider may perform only the type of Program Service that is registered to perform.

A corporate affiliate of a Customer that is Owned and Controlled by the Customer or by the Customer's ultimate parent and which performs Program Service exclusively for the Customer and not for any other Customer is deemed not to be a Service Provider. The Customer must ensure that any person performing Program Service that directly or indirectly supports or otherwise benefits the Customer's Program(s), and whether or not such person is registered by the Corporation as a Service Provider:

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

For the avoidance of doubt: Program Service in support of or otherwise benefitting an Affiliate Program(s) is deemed to be Program Service in support of or otherwise benefitting the Program(s) of the Principal that Sponsors such Affiliate.

14.3 General Obligations

Each Service Provider and each Customer that registers a Service Provider must comply with all of the following.

14.3.1 Program Responsibility and Control

A Customer must at all times be entirely responsible for and must manage, direct, and control all aspects of its Programs and the Program Service performed by Service Providers, and establish and enforce all Program management and operating policies in accordance with the Standards. A Customer must not transfer or assign any part or all of such responsibilities or in any way limit its responsibility with regard to its Service Providers. A Customer must conduct meaningful monitoring of its Programs and Activities to ensure ongoing compliance by its Service Providers with applicable Standards.

14.3.2 Notification to and Registration by the Corporation

Each Principal must advise the Corporation promptly when any of its Service Providers ceases to perform Program Service in connection with the Customer's Program(s) or undergoes a change of name or transfer of Ownership or Control.

Each Type I TPP must advise the Corporation promptly and directly in writing when it:

1. Commences to perform or ceases to perform Program Service for any Customer, and on an ongoing basis, inform the Corporation of all ICA numbers pertaining to for which it is performing any Program Service;
2. Undergoes a change of name or transfer of Ownership or Control;
3. Fails or refuses to make payments in the ordinary course of business;
4. Makes an assignment for the benefit of creditors; or
5. Seeks bankruptcy protection or similar protection.

A Customer may not receive Program Service by or from any person other than as set forth in the Standards.

14.3.3 Program Service Agreement

This Rule 14.3.3 is not applicable with respect to a Service Provider whose provision of Program Service to the Customer consists only of DSE Program Service.

Prior to the commencement of the performance of Program Service by a person in support of a Customer Program, the Customer and the Service Provider must enter into a written agreement describing the Program Service to be performed (the "Program Service agreement"). The Program Service agreement must be updated from time to time as appropriate to reflect the Program Service that the Service Provider performs in support of or otherwise benefitting, directly or indirectly, the Customer Program(s) and may not contradict, or be inconsistent with, the Standards.

The Program Service agreement must reflect the Customer's responsibility, as described in this chapter, for establishing all management and operating policies and must not include any provision that limits, or attempts to limit, the Customer's responsibility for the Program. The Program Service agreement must, in substance, include all of the following provisions:

1. The Service Provider received, understands, and agrees to comply with all applicable Standards, including the Service Provider Rules.
2. On an ongoing basis, the Service Provider is promptly to provide the Customer with the current addresses of each of its offices.
3. In the event of any inconsistency between any provision of the Program Service agreement and the Standards, the Standards will govern.

4. The Program Service agreement automatically and immediately terminates if the Corporation de-registers the Service Provider or if the Customer ceases to be a Customer for any reason or if the Customer fails to have a valid License by the Corporation to use any Mark pertaining to the Program Service to be performed by the Service Provider.
5. The Service Provider acknowledges and agrees:

    a. to comply with all Standards, as amended from time to time, applicable to the Program Service to be provided;

    b. that the Corporation is the sole and exclusive owner of the Marks;

    c. not to contest the ownership of the Marks for any reason;

    d. the Corporation may at any time, immediately and without advance notice, prohibit the Service Provider from using any of the Marks for any reason;

    e. the Corporation has the right to enforce any provision of the Standards and to prohibit an Service Provider from engaging in any conduct the Corporation deems could injure or could create a risk of injury to the Corporation, including injury to reputation, or that could adversely affect the integrity of the Interchange System, the Corporation's Confidential Information as defined in the Standards, or both; and

    f. the Service Provider will not take any action that could interfere with or prevent the exercise of this right by the Corporation.

14.3.3.1 Before Entering into a Program Service Agreement with a Service Provider

Before entering into, extending, or renewing a Program Service Agreement, a Customer must verify that the Service Provider is a bona fide business, has sufficient safeguards in place to protect Account data from unauthorized disclosure or use, and complies with applicable laws.

In determining whether the Service Provider is a bona fide business, the Customer must verify, at a minimum, all of the following have been completed:

1. credit check, background investigations, and reference checks of the Service Provider. If the credit check of the Service Provider raises questions or does not provide sufficient information, the Customer should also conduct a credit check of:

    a. the owner(s) of the Service Provider, if the Service Provider is a sole proprietor;

    b. the partners that together own or control the Service Provider, if the Service Provider is a partnership; or

    c. the principal shareholders that together own or control the Service Provider, if the Service Provider is a corporation.

2. inspection of the Service Provider's premises and records to ensure that the Service Provider has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, the appropriate license or permit and other capabilities to conduct business. If the Service Provider conducts or plans to conduct business in more than one set of premises, the Customer must inspect at least one of them.

The Corporation does not require a Customer 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 that the Customer reviews, and finds satisfactory for the purposes of the Program Service being considered, the Service Provider's most recent annual report, 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 revenue exceeds USD 50 million.

The Customer must retain all records concerning the investigation of any Service Provider with which it has entered into a Program Service agreement for a minimum of two years after the date the agreement is terminated or expires.

14.3.4 Disclosure of Standards

Before a Customer proposes a person to be registered as a Service Provider by the Corporation, the Customer must provide the proposed Service Provider with a copy of the Standards then in effect applicable to Service Providers and Program Service the proposed Service Provider is expected to perform, including these Service Provider Rules. After registration, the Customer must promptly provide a Service Provider with any change to the Standards applicable to such Program Service, including any change to these Service Provider Rules.

14.3.5 Customer Point of Contact

A Service Provider must promptly provide a name or title of, and a telephone number for a contact person of the Customer:

1. upon request by a Cardholder, Merchant, or an ATM site owner, or
2. if the Service Provider is unable or unwilling to respond to a question to the Cardholder's, Merchant's or ATM site Owner's satisfaction.

14.3.6 Affiliate

Program Service performed in support of an Affiliate's Program(s) is deemed to be performed in support of the Program(s) of the Principal that Sponsors the Affiliate. For that reason, an Affiliate wishing to receive Program Service from a Service Provider must obtain the prior written consent of the Affiliate's Sponsoring Principal(s).

14.3.7 Use of the Marks

A Service Provider must not use any Mark on its own behalf, whether in connection with Program Service or otherwise. The Service Provider may not suggest or in any manner create an impression that the Service Provider is a Customer or a representative of the Corporation, or that the Service Provider is anything other than a Service Provider of the Customer. The Service Provider must not create an impression that the Corporation in any way endorses the Service Provider or the Program Service the Service Provider performs.

The Service Provider may use one or more of the Marks in connection with the Program Service it performs, provided:

1. the Marks are used in accordance with the Standards, including all reproduction, usage, and artwork Standards that may be in effect from time to time;
2. the Marks are used according to the express written instructions of the Customer; and
3. the Marks are used solely in connection with the provision of Program Service.

The Service Provider may use the Marks on its stationery, letterhead, or business cards only if accompanied, in close proximity, by a clear statement that identifies the Service Provider as an agent for a Customer and that includes the Customer's name by which the Customer identifies itself to the public (for example, "Service Provider is an authorized representative of Bank XYZ").

14.3.8 Service Provider Identification on a Card

The name of a non-Customer Service Provider may appear on a Card only if that Service Provider does not provide acquiring Program Service for or in connection with any Customer Program or Activity.

14.3.9 Program Materials

A Customer must approve all Program documents and other materials before any distribution, disclosure or other use thereof by a Service Provider. The Program materials may not state or imply that the Service Provider is participating in, or conducting any activity not expressly permitted by the Standards. Program materials include, by way of example, Merchant applications, Card applications, Merchant Agreements, ATM deployment agreements, Cardholder agreements, Merchant statements, Cardholder statements, marketing materials and Cardholder Communications, including Solicitations.

14.3.10 Fees

A Customer must approve, in advance, any fee or other obligation associated with the Customer's Program and a Service Provider may not collect or attempt to collect any such fee or obligation without the express prior written approval of the Customer. Any fee must be clearly and conspicuously disclosed in writing to the Merchant or Card applicant, as appropriate, prior to any request or demand for payment of the fee.

14.3.11 Settlement Account

A Service Provider must not have access to any account for funds then or subsequently due to a Merchant for Activity and/or funds withheld from a Merchant for chargebacks arising out of Activity. A Customer must not assign or otherwise transfer an obligation to pay or reimburse a Merchant to a Service Provider if the obligation arises from Activity.

14.3.12 Transfer of Rights Prohibited

A Service Provider must not subcontract, sublicense, assign, license, franchise, or in any other manner extend or transfer to any third party any right or obligation the Service Provider may have in connection with performing Program Service for a Customer, and any such transfer is null and void. A Service Provider may perform Program Service to a Customer only using the Service Provider's own employees or employees of a different Service Provider that is confirmed also to be registered by the Corporation to provide Program Service for that same Customer.

14.3.13 Use of Systems and Confidential Information

A Service Provider performing Program Service and each Service Provider Registration Facilitator must agree to:

1. use any of the Corporation's equipment and software ("Systems"), including but not limited to any MasterCard Interface Processor (MIP) or Network Interface Processor (NIU) used to connect to the Interchange System, and any of the Corporation's information identified or reasonably understood to be confidential or proprietary ("Corporation's Confidential Information") solely in order to perform its duties on behalf of the Customer and not for any other purpose;
2. treat the Systems and Corporation's Confidential Information in at least as careful and confidential a manner as the Service Provider treats its own and the Customer's systems and proprietary information;
3. acknowledge that access to the Systems and Corporation's Confidential Information does not provide the Service Provider with any right, title, interest, or copyright therein or any license to use, sell, exploit, copy, or develop them further;
4. limit access to the Systems and Corporation's Confidential Information to those Service Provider employees with a need to have access or to know in order to enable the Service Provider to perform Program Service and to implement and to maintain reasonable and appropriate safeguards to prevent unauthorized access to the Systems or disclosure of Corporation's Confidential Information;
5. immediately cease any and all use of the Systems and Corporation's Confidential Information upon request of the Corporation or the Customer or upon the earlier termination or completion of the Service Provider's performance of Program Service, and to immediately deliver all Systems and Corporation's Confidential Information to the Corporation;
6. immediately advise the Customer and the Corporation if any unauthorized person seeks access to the Systems or Corporation's Confidential Information, whether by legal proceedings or otherwise.

The obligations set forth in this Rule 14.3.13 survive the termination or expiration of the Program Service agreement.

14.3.14 Indemnification

Program Service performed by any person or entity, which Program Service directly or indirectly supports or otherwise benefits a Customer's Program(s), and regardless of whether such person or entity is or was registered with the Corporation as a Service Provider or is itself a Customer, is Activity and thereby subjects the Customer to the indemnification and other obligations set forth in Rule 13.14 of this rulebook.

14.3.15 No Endorsement of the Corporation

In no event does compliance with these Service Provider Rules or enforcement or any lack of or delay in enforcement thereof or the registration of a Service Provider imply, suggest, or otherwise mean that the Corporation endorses any Service Provider or the nature or quality of Program Service or other performance or that the Corporation approves of, is a party to, or a participant in, any act or omission by a Service Provider or other entity acting for or on behalf of a Customer.

14.3.16 Audits

The Corporation or its designee may conduct one or more regular or periodic financial and procedural audits of the Customer, its Service Provider(s), or both, at any time and from time to time for the purpose of determining compliance with the Standards, including these Service Provider Rules. The Customer bears all costs of any such audit or audits. The Customer and its Service Provider(s) each must fully co-operate with and promptly supply the Corporation with all information and material upon request.

14.3.17 Settlement Failure Obligation

A Service Provider that becomes aware of a settlement failure by the Customer(s) for which the Service Provider performs Program Service must promptly, and in no event later than twenty-four (24) hours after becoming aware of such failure, notify the Corporation in writing of such failure.

14.3.18 Data Security

A Service Provider must comply with all Standards pertaining to the storage, and/or safeguarding, and/or transmission, of Card and Transaction data.

If a Service Provider reasonably believes that an unauthorized person accessed or may have accessed Account, Cardholder, or Transaction information in the possession or control of the Service Provider or any other third party, the Service Provider must promptly notify the Customer(s) for which it performs Program Service in writing of such belief and the Customer must promptly notify the Corporation in writing of such belief.

14.4 Acquiring Programs

In addition to complying with the general obligations set forth in Rule 14.3 above, each Customer and each Service Provider that perform Program Service with respect to that Customer's acquiring Programs also must comply with the Standards set forth in this Rule 14.4.

14.4.1 Merchant Agreement

The Merchant Agreement establishing the terms of an acquiring relationship between the Acquirer and a Merchant must:

1. Be signed by the Customer with no separate or other agreement between the Service Provider and the Merchant regarding Activity. The Service Provider may be a party to the Merchant Agreement, in which case the Merchant Agreement must contain the substance of all of the following:

   a. For purposes of this Merchant Agreement and performance of the Merchant Agreement by the Service Provider, (i) the Service Provider is the exclusive agent of the Customer; (ii) the Customer is at all times and entirely responsible for and in control of Service Provider performance; and (iii) the Customer must approve, in advance, any fee payable to or obligation of the Merchant arising from or related to performance of the Merchant Agreement.

   b. The Merchant Agreement is not effective and may not be modified in any respect without the express written consent of the Customer.

   c. The Service Provider may not have access, directly or indirectly, to any account for funds or funds due to a Merchant and/or funds withheld from a Merchant for chargebacks arising from, or related to, performance of this Merchant Agreement. The Customer may not assign or otherwise transfer an obligation to pay or reimburse a Merchant arising from, or related to, performance of the Merchant Agreement to a Service Provider

   d. The Service Provider may not subcontract, sublicense, assign, license, franchise, or in any manner extend or transfer to any third party, any right or obligation of the Service Provider set forth in the Merchant Agreement. The Customer may not waive, forgive, release, assign, or fail to insist on strict performance of each requirement set forth in these parts (a.) through (d).

2. Confirm the Customer's responsibility for the Program and for the Merchant's Program participation and confirm that the Merchant Agreement does not contain any provision that could be deemed to limit such responsibility.

3. Not take effect or state or imply that it takes or has taken effect prior to being signed by the Customer.

4. Disclose the Customer's name and sufficient information to enable the Merchant to contact the Customer directly by telephone or in writing.

Refer to Chapter 7, "Acquiring" for more information about Merchant Agreements.

14.4.2 Collection of Funds

Discount rates (or similar charges called by other terms) due to a Customer from a Merchant must be collected directly by the Customer and not by the Service Provider.

14.4.3 Access to Documentation

The Customer at all times must maintain prompt and unrestricted physical access to all original, executed Merchant Agreements and completed ATM and Merchant site inspection reports. The Customer must forward true and complete copies of any one or more of these documents to the Corporation promptly upon request.

14.4.4 Authority to Terminate Merchant Agreement and ATM Deployment Agreement

A Customer may not limit or in any manner condition its authority to terminate any Merchant Agreement or ATM deployment agreement to accommodate a Service Provider or otherwise.

14.5 Card Issuing Programs

In addition to complying with the general obligations set forth in Rule 14.3 of these Service Provider Rules, each Customer and each Service Provider that performs Program Service with respect to that Customer's Card issuing Program also must comply with the Standards set forth in this Rule 14.5.

14.5.1 Card Applicant Approval

The Customer itself, and not a Service Provider, must approve of a Card applicant's participation in a Card Program.

14.5.2 Cardholder Agreement

The Cardholder agreement must disclose the Customer's name and sufficient information to enable the Cardholder to contact the Customer directly by telephone or in writing. The Service Provider must not be a party to the Cardholder agreement.

14.5.3 Payment of Fees

All Program payments other than application fees for initial Program participants must be collected directly by the Customer and not by the Service Provider.

14.5.4 Program Receivables

A Service Provider may own Program receivables or participate in a financing vehicle involving Program receivables so long as the Corporation determines that the Customer continues to own and control the Program. Ownership of Program receivables by the Service Provider does not in any way limit the Customer's obligation to comply with the Standards.

14.6 Service Provider Registration

14.6.1 Registration Requirements for DSEs, ISOs, and Type II TPPs

Each Principal, for itself and each of its Sponsored Affiliates must use the MasterCard Registration Program (MRP) system on MasterCard Connect to register any Service Provider not designated by the Corporation as a Type 1 TPP. A Customer may elect to register a person as an SPRF for the purpose of having that SPRF perform Service Provider registration requirements for DSE, ISO, and Type II SPP Service Providers on the Customer's behalf.

1. The Principal must submit all information and material required by the Corporation in connection with the proposed registration within 60 days of the registration application submission date.
2. A Service Provider performing TPP Program Service that also wants to provide ISO Program Service to one or more Customers must be distinctly proposed for registration by the Corporation on behalf of each Customer that wants to receive Program Service from that Service Provider
3. A Service Provider that performs services involving the storage, transmission, or processing of Card or Transaction data must comply with the MasterCard Site Data Protection (SDP) Program in accordance with the implementation schedule set forth in Rule 8.10.5 of this rulebook. Before initiating registration, the Customer must instruct the Service Provider to contact the Corporation via e-mail at sdp@mastercard.com and validate its compliance with the SDP Program using the tools described in Rule 8.10.2 of this rulebook. For any proposed Type II TPP that is not compliant, the Customer or TPP must provide a Corporation-approved compliance action plan. A Corporation-approved compliance action plan does not exempt the Principal from responsibility and liability that arises from the Principal's or any of its Sponsored Affiliates' or their Type II TPP's noncompliance with any Standard, including those relating to the disclosure and securing of Card, Cardholder, and Transaction data. The registration of a proposed DSE will not be deemed complete until its compliance with the SDP Program is validated.
4. The Corporation collects the appropriate fee(s) then in effect from the Customer that proposes the registration via the MasterCard Consolidated Billing System (MCBS).
5. The Principal must receive the Corporation's written or e-mail confirmation of the registration before the Principal or any of its Sponsored Affiliates receives Program Service from an ISO or Type II TPP or any of their Service Providers or Merchants receive Program Service from a DSE and before the Service Provider commences performing such Program Service or represents itself to any person as authorized to provide such Program Service on behalf of the Principal or any of its Sponsored Affiliates. In its sole discretion, the Corporation may approve or may reject any application for the registration of a Service Provider.

6. To maintain the registration of a Service Provider, the Customer must submit such information and material as may be required by the Corporation from time to time, including but not limited to a copy of the Program Service agreement, if applicable. The renewal fee then in effect is debited from the Customer via MCBS. In its sole discretion, the Corporation may decline to renew the registration of a Service Provider.

If the Customer terminates a Service Provider, the Customer must notify the Corporation or its SPRF of the termination date and of the reasons for the termination. This notification must be received by the Corporation or its SPRF within one week of the decision to terminate. In its sole discretion, the Corporation may require a Customer to terminate a Service Provider at any time.

14.6.1.1 SDP Program Noncompliance

Each Principal that has registered or proposed the registration of a Type II TPP to perform Program Service for it and/or for any one of its Sponsored Affiliates must promptly notify each of its Merchants and other customers that directly or indirectly are or may benefit from or may otherwise be impacted, as the case may be, by the Program Service if the registered or proposed TPP is not or will not be fully compliant with SDP Program requirements applicable to it as a TPP by and after the date performance of the Program Service commences. Such notification must include, with respect to the registered or proposed TPP:

- The name and address of the TPP;
- A description of the Program Service to be or being provided by the TPP;
- A description of SDP Program requirements the TPP is not compliant with; and
- A specific date by which the TPP will become fully compliant with applicable SDP Program requirements, or, in the alternative, the date by which the TPP will cease performing Program Service.

The application of a DSE will not be approved until such time as the DSE becomes fully compliant with SDP Program requirements.

14.6.2 Registration Requirements for Type I TPPs

A TPP that the Corporation designates as a Type I TPP, upon receiving notification of such designation, must apply to be registered by the Corporation as a Type I TPP and must be registered by the Corporation as a Type I TPP Service Provider before commencing to provide TPP Program Service. A Type I TPP that also wishes to provide ISO Program Service to one or more Customers must be distinctly proposed to the Corporation or a Service Provider Registration Facilitator (SPRF) for registration by each Customer wishing to receive ISO Program Service from that Type I TPP.

Post-registration by the Corporation of a Type I TPP, on a quarterly basis, the applicable fee is charged by the Corporation directly to the Type I TPP. Renewal of Type I TPP registration status is at the sole discretion of the Corporation.

14.6.3 Registration of a Service Provider Registration Facilitator

A Customer itself must request that a person be registered by the Corporation as a Service Provider Registration Facilitator ("SPRF") and a person must be registered by the Corporation as an SPRF before commencing to provide Service Provider Registration Program Service.

14.6.4 Service Provider Registration Noncompliance

A Principal that fails to comply with these Service Provider registration requirements, including the failure to complete a Service Provider registration within sixty (60) days as set forth in Rule 14.6.1 of this rulebook, is subject to noncompliance assessments of up to USD 25,000 for each thirty (30)-day period of noncompliance.

14.6.5 Prohibition from Acting as a Service Provider

The Corporation reserves the right to prohibit, either for a fixed period of time or permanently, a Service Provider, its owners, officers, and/or employees from performing Program Service, acting as a DSE, or both.

14.6.6 Termination of Program Service Agreement or De-registration

On the effective date of the termination or expiration of the Program Service agreement(s), or upon notice by the Corporation, or upon de-registration of a person as a Service Provider, the person must immediately cease all use of the Corporation's systems and Marks, and must cease performing Program Service.

14.7 Type I TPP Evaluation Program

14.7.1 Compliance with Type I TPP Evaluation Program Standards

Each Type I TPP is required to comply with the Type I TPP Evaluation Program requirements and fully cooperate with any effort by the Corporation to determine such compliance. The Corporation requires all Type I TPPs to participate fully in each such review.

14.8 Confidential Information of Service Providers

The Corporation will not disclose confidential information furnished to it by a Customer or Service Provider pursuant to these Service Provider Rules, except to the Customer or Service Provider supplying the information, or as part of a general statistical compilation that does not reveal individual Customer or Service Provider data, or as may be required by any court process or governmental agency having or asserting jurisdiction over the Corporation, or as otherwise described in Rule 3.7.2 of this rulebook.

The registration and Type I TPP Evaluation Program compliance status of a Type I TPP, including the identity of the Customer(s) for which the Type I TPP performs Program Service, the nature of Program Service the Type I TPP performs, and the results of any Type I TPP evaluation are not confidential information.

The identities of a Service Provider Registration Facilitator and the Customer(s) for which the Service Provider Registration Facilitator performs registration services are not confidential information.

In addition, and notwithstanding the aforesaid, as a condition of the registration or renewal of registration of a Service Provider, the Customer and Service Provider each agree that the Corporation may disclose such information of and about the Customer and Service Provider as the Corporation deems necessary or appropriate.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
14.1 Service Provider Categories	A
14.3.1 Program Responsibility and Control	A
14.3.2 Notification to and Registration by the Corporation	A
14.3.3 Program Service Agreement	A
14.3.4 Disclosure of Standards	C
14.3.5 Customer Point of Contact	B
14.3.6 Affiliate	A
14.3.7 Use of the Marks	B

Rule Number/Rule Title	Category
14.3.8 Service Provider Identification on a Card	B
14.3.9 Program Materials	B
14.3.10 Fees	B
14.3.11 Settlement Account	A
14.3.12 Transfer of Rights Prohibited	A
14.3.13 Use of Systems and Confidential Information	A
14.3.16 Audits	B
14.3.17 Settlement Failure Obligation14.3.17 Settlement Failure Obligation	A
14.3.18 Data Security	A
14.4.1 Merchant Agreement	A
14.4.2 Collection of Funds	A
14.4.3 Access to Documentation	B
14.4.4 Authority to Terminate Merchant Agreement and ATM Deployment Agreement	B
14.5.1 Card Applicant Approval	A
14.5.2 Cardholder Agreement	B
14.5.3 Payment of Fees	A
14.5.4 Program Receivables	A
14.6 Service Provider Registration	A
14.7.1 Compliance with Type I TPP Evaluation Program Standards	A

Chapter 15 Asia/Pacific Region

This chapter contains Rule variations or additional Rules applicable only to the Asia/Pacific Region.

Overview

Set forth below are the Rule variations to the *Maestro Global Rules* and additional Rules for the Asia/Pacific Region. In most cases, the Asia/Pacific chapter supplements part 1 of this rulebook and Asia/Pacific Customers must comply with the Rules in both part 1 and Chapter 15, "Asia/Pacific Region," of this rulebook.

If a subsection in the Asia/Pacific regional chapter contains the full set of Rules applicable to Asia/Pacific Customers, in place of the corresponding chapter in part 1 of this rulebook, then this is clearly mentioned, and Asia/Pacific Customers are required to comply only with the Rules in that Asia/Pacific chapter.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

Definitions

In addition to the defined terms in the "Definitions," chapter in part 1 of this rulebook, the following applies:

Competing International ATM Network

A network of ATMs and access cards, other than the Corporation, identified by a common brand mark that is used exclusively or primarily for ATM interchange and that possesses each of the following characteristics:

- it operates in at least three (3) countries;
- it uses a common service mark or common service marks to identify the terminals and cards which provide account access through it;
- there are at least forty million (40,000,000) debit cards that provide account access through it; and
- there are at least twenty-five thousand (25,000) ATMs that provide account access through it.

1.1 Types of Customers

In addition to the Rules in Chapter 1, "Participation," Rule 1.1 in part 1 of this rulebook, the following apply:

A Customer may participate in one of the following categories:

1. **Full Customer:** A Full Customer is a financial institution that issues Cards and acquires Transactions.
2. **Issuing Customer:** An Issuing Customer is a financial institution that issues Cards but does not acquire Transactions.
3. **Acquiring Customer:** An Acquiring Customer is a financial institution or an entity eligible under Rule 1.2. (5.b), of part 1 of this rulebook that acquires Transactions but does not issue Cards. This type of Customer is also referred to as an "Acquiring-only" Customer in this rulebook.

All Customers are deemed to be Principals, unless they are accepted by the Corporation as Affiliates (formerly known in the Region as "Sponsored Customers").

Principals, regardless of whether they are Full Customers, Issuing Customers, or Acquiring Customers, may Sponsor Customers in all categories of License, i.e., Full Customers, Issuing Customers and Acquiring Customers.

1.3 Application to be a Customer

In addition to the rules in Chapter 1, "Participation, Rule 1.3.1 in part 1 of this rulebook, the following apply:

In the event that:

4. an Issuing Customer or an Acquiring Customer wishes to become a Full Customer; or

5. a Full Customer wishes to become only an Issuing Customer or an Acquiring Customer.

1.6 Obligations, Rights and Responsibilities

1.6.7 Additional Rules for Participation

With the exception of Issuers in American Samoa, Guam, and Northern Mariana Islands, Customers must not participate as an Issuer of debit cards in any Competing EFT POS Network. A Customer, including a Customer in American Samoa, Guam, and Northern Mariana Islands, must not participate as an Issuer of debit cards in any Competing International ATM Network.

1.7 Termination of License

1.7.3 Automatic Termination of the Right to Participate

In addition to the Rules in Chapter 1, "Participation," Rule 1.7.3 in part 1 of this rulebook, the following applies:

9. the Customer merges, combines, or consolidates with another entity that is not a Customer.

1.7.4 Liabilities and Obligations Following Termination

The following replaces Chapter 1, "Participation," Rule 1.7.4 (3 and 4), in part 1 of this rulebook:

3. must cease all use of the Marks and will reissue replacement debit cards or other access devices which do not display the Marks within ninety (90) days of the termination date;

In addition to the Rules in Chapter 1, "Participation," Rule 1.7.4 in part 1 of this rulebook, the following applies:

4. must immediately give notice of its termination to any Merchants it has authorized to honor Cards. If any Merchant connected to a terminating or resigning Customer wishes to continue to participate in the Program, such Customer must cooperate with the Corporation and other Customers in facilitating the transfer of such Merchant to another Customer.

4.2 Protection and Registration of the Marks

In addition to the Rules in Chapter 4, "Marks," Rule 4.2 in part 1 of this rulebook, the following applies to Cards issued in American Samoa, Guam, and Northern Mariana Islands:

No use of a Mark may be made on or in connection with any card, device or other application associated with a payment service that the Corporation deems to be competitive with any Activity except as set forth in this chapter.

4.5 Display on Cards

In American Samoa, Guam and Northern Mariana Islands, the following replaces the second paragraph of Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook:

The Marks may be placed on a card in combination with other local/regional/international POS debit marks and/or local/international ATM marks. In the event that a card has an international POS debit mark on the card front, and the card has a Maestro payment application:

1. if any other POS debit mark appears on the card back, the Marks must be displayed on the card back; or
2. if no other POS debit mark appears on the card back, the Marks are not required to appear on the card back.

A card must not include any visible indication communicating that acceptance or use of the Mark or the Maestro payment application is limited, geographically or otherwise.

The fifth paragraph of Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook in which Customers are prohibited from placing any other Competing EFT POS Network debit marks on their participating Cards does not apply to Cards issued in American Samoa, Guam, or the Northern Mariana Islands.

6.4 PIN and Signature Requirements

6.4.3 Use of PIN or Signature

In addition to the Rules in Chapter 6, "Issuing," Rule 6.4.3 in part 1 of this rulebook, the following applies:

PIN entry is required for all intraregional Transactions.

6.13 Issuer Responsibilities to Cardholders

In addition to the Rules in Chapter 6, "Issuing," Rule 6.13 in part 1 of this rulebook, the following apply:

1. **Card Applications and Card Solicitations**. Each Issuer of Cards shall disclose, clearly and conspicuously, in all Card applications and Card Solicitations any amounts in respect to the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
2. **Cardholder Agreements and Account Agreements**. Each Issuer of Cards shall disclose, clearly and conspicuously, in all existing Cardholder agreements and Account agreements amounts in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
3. **Periodic Billing Statement**. Each Issuer of Cards shall provide adequate disclosure on each applicable periodic billing statement, such that the Cardholder can readily determine from the billing statement any amounts that the Issuer charges to the Cardholder in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment during that billing cycle, either in gross or on a per Transaction basis.
4. **Currency Conversion Procedure**. The Corporation further recommends and encourages Customers to inform their Cardholders that part of the Corporation currency conversion procedure includes use of either a government-mandated exchange rate or a wholesale exchange rate, selected by the Corporation, and that the government-mandated exchange rate or wholesale exchange rate that the Corporation uses for a particular Transaction is the rate the Corporation selects for the applicable currency on the day the Transaction is processed, which may differ from that applicable to the date the Transaction occurred or when it is posted to the Cardholder's Account.

NOTE

Refer to the *Single Message System Specifications* for additional information about the MasterCard Currency Conversion Assessment. For information about the MasterCard Cross-border Assessment, refer to the *MasterCard Consolidated Billing System—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," Rule 7.2 in part 1 of this rulebook, the following applies:

14. 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.

7.2.3 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:

1. previously owed to the Merchant; or
2. 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.

7.9 POS Terminal and Terminal Requirements

7.9.2 Manual Key-Entry of PAN

The following replaces Chapter 7, "Acquiring," Rule 7.9.2 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.

7.11 Additional Requirements for POS Terminals

In addition to the rules in Chapter 7, "Acquiring," Rule 7.11 in part 1 of this rulebook, the following applies:

3. POS Terminals must contain keyboards that assign letter-number combinations as described in Rule 7.12 in part 1 of this rulebook.

7.17 Connection to the Interchange System

7.17.1 ATM Connection to the Interchange System

The following replaces paragraph 2 of Chapter 7, "Acquiring," Rule 7.17.1 in part 1 of this rulebook:

Customers that acquire Transactions must make available for connection to the Interchange System at least seventy-five percent (75%) of their eligible ATMs within one (1) year of the approval of its application for a License.

7.17.2 POS Terminal Connection to the Interchange System

Customers that acquire Transactions must make available for connection to the Interchange System at least seventy-five percent (75%) of their eligible POS Terminals within one (1) year of the approval of its application for a License.

7.18 Card Capture

7.18.1 POS Transactions

In addition to the second paragraph of Chapter 7, "Acquiring," Rule 7.18.1 in part 1 of this rulebook, the following applies:

The capture of Cards at POS Terminals is prohibited.

7.23 ATM Access Fees

7.23.1 Domestic Transactions

The following replaces Chapter 7, "Acquiring," Rule 7.23.1, paragraph 1 in part 1 of this rulebook:

For the purposes of this Rule 7.23.1, "ATM Access Fee" shall mean a fee charged by an Acquirer in Australia in connection with any financial or non-financial Transaction initiated at that Acquirer's ATM with a Card, which fee is added to the amount of the Transaction transmitted to the Issuer.

Upon complying with the ATM Access Fee notification requirements of the Rules, Acquirers in Australia may assess an ATM Access Fee on a Transaction initiated with a Card that was issued in Australia so long as the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory fashion.

7.23.2 Cross-border Transactions

7.23.2.1 Transaction Field Specifications

At the time of each Transaction on which an ATM Access Fee is imposed, the Acquirer of such Transaction must transmit the amount of the ATM Access Fee in the field specified in the *Single Message System Specifications* manual or the Regional Service Center manual applicable to the Transaction message format.

7.23.2.2 Non-Discrimination Regarding ATM Access Fees

An Acquirer must not charge an ATM Access Fee in connection with a Transaction that is greater than the amount of any ATM access fee charged by that Acquirer in connection with the transactions of any other network accepted at that Terminal.

7.23.2.3 Notification of ATM Access Fee

An Acquirer that plans to add an ATM Access Fee must notify its Sponsoring Principal, in writing, of its intent to do so before the planned first imposition of such ATM Access Fee by the Acquirer.

The Principal must update the Location Administration Tool (LAT) regarding its or its Affiliates' imposition of ATM Access Fees.

7.23.2.4 Cancellation of Transaction

Any Acquirer that plans to add an ATM Access Fee must notify the Cardholder with a screen display that states the ATM Access Fee policy and provides the Cardholder with an option to cancel the requested Transaction.

7.23.2.5 Terminal Signage, Screen Display, and Transaction Record Requirements

An Acquirer that plans to add an ATM Access Fee on a Transaction must submit proposed Terminal screen display and receipt copy that meets the requirements of the Rules to its Sponsoring Principal in writing for approval before use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook).

In addition, if the Acquirer displays Terminal signage, the Acquirer must submit proposed Terminal signage copy that meets the requirements of the Rules to its Sponsoring Principal in writing for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen and Receipt Text Displays," in part 2 of this rulebook).

The Sponsoring Principal has the right to determine the acceptability of any new or changes to previously approved Terminal signage, screen display, and receipt copy. In cases of conflict between an Acquirer and its Sponsoring Principal, the Corporation has the sole right to determine the acceptability of any and all Terminal signage, screen display, and receipt copy.

7.23.2.5.1 Additional Requirements for Terminal Signage

An Acquirer that plans to add an ATM Access Fee to a Transaction may optionally display signage that is clearly visible to Cardholders on or near all Terminals at which ATM Access Fees apply.

The minimum requirement for ATM Access Fee Terminal signage text is wording that clearly states:

1. the name of the ATM Owner and Principal;
2. that the Transaction may be subject to an ATM Access Fee that will be deducted from the Cardholder's Account in addition to any Issuer fees;
3. the amount of, calculation method of, or Corporation-approved generic signage regarding the ATM Access Fee;
4. that the ATM Access Fee is assessed by the Acquirer instead of the Issuer; and
5. that the ATM Access Fee is assessed on intracountry Transactions only.

The minimum requirements for Terminal signage (physical characteristics) are as follows:

1. the signage must bear the heading "Fee Notice";
2. the size of the Terminal signage must be a minimum of four (4) inches in height by four (4) inches in width;
3. the text must be clearly visible to all. It is recommended that the text be a minimum of fourteen (14) point type;
4. the heading must be clearly visible to all. It is recommended that the text be a minimum of eighteen (18) point type.

A model for Terminal signage regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.2.5.2 Additional Requirements for Terminal Screen Display

An Acquirer that plans to add an ATM Access Fee on a Transaction must present a screen display message that is clearly visible to Cardholders on all Terminals at which ATM Access Fees apply. If the Cardholder is given the option of choosing a preferred language in which to conduct the Transaction, the screen display message concerning ATM Access Fees must be presented to the Cardholder in that chosen language.

If an Acquirer displays the Corporation-approved generic ATM Access Fee signage, the Acquirer must include the amount of the ATM Access Fee as part of the Terminal screen display.

A model for the Terminal screen display regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.2.5.3 Additional Requirements for Transaction Records

An Acquirer that adds an ATM Access Fee on a Transaction must make available to the Cardholder on its Terminal receipt the ATM Access Fee information required by this Rule 7.23.2.5.3, in addition to any other information the Acquirer elects or is required to provide.

The minimum requirements for the Terminal receipt are:

1. a statement of the amount disbursed to the Cardholder;
2. a statement of the ATM Access Fee amount with language clearly indicating it is a fee imposed by the Acquirer;
3. a separate statement of the combined amount of the ATM Access Fee and the disbursed amount, with language clearly indicating that this amount will be deducted from the Cardholder's Account.

A model for Terminal receipt text regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.24 Return Merchandise Adjustments, Credits, and Other Specific Terms of a Transaction

With proper disclosure at the time of any Transaction, a Merchant:

1. is not obliged to accept merchandise in return or exchange or to issue refunds to Cardholders;
2. may only accept merchandise in immediate exchange for similar merchandise of a price equal to the amount of the original Transaction;
3. 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;
4. if permitted by applicable law, may stipulate special circumstances agreed to by the Cardholder, *e.g.*, late delivery charges, insurance charges; or
5. 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 (1)—"NO REFUND" as related to paragraph (2)—"EXCHANGE ONLY" as related to paragraph (3)—"IN-STORE CREDIT ONLY" as related to paragraph (4)—(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.

9.2 POS Transaction Types

9.2.1 Issuer Online POS Transactions

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.1 in part 1 of this rulebook, the following applies:

11. balance inquiry.

9.2.2 Acquirer Online POS Transactions

9.2.2.1 Required Transactions

The following replaces Chapter 9, "Processing Requirements," Rule 9.2.2.1 (1) in part 1 of this rulebook:

1. Purchase from primary account. (Purchase from account selection from checking and savings account is optional).

9.2.2.2 Optional Online POS Transactions

The following replaces Chapter 9, "Processing Requirements," paragraph 4 of Rule 9.2.2.2 (1.d) 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 Interchange System and the Issuer.

9.8 Authorizations

9.8.2 Transaction Routing

For the avoidance of doubt, Rule 9.8.2 of Chapter 9, "Processing Requirements" of this rulebook does not inhibit a Merchant's ability to direct the routing of a transaction conducted in American Samoa, Guam, or Northern Mariana Islands with a Card that is issued in the United States Region, American Samoa, Guam, Northern Mariana Islands, Puerto Rico or U.S. Virgin Islands to any debit payment network enabled on the Card.

13.8 Pre-authorized Transactions

The following replaces Chapter 13, "Liabilities and Indemnification," paragraph 1 of Rule 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.

13.10 Manually-entered PAN

An Issuer is not liable to the Acquirer for Transactions completed at a Merchant through manual entry of a PAN that is accepted by the Issuer and subsequently determined to have been generated through use of a fraudulent Card and/or unauthorized use of a PIN.

13.19 Liability of Affiliates

Except to the extent any liability or obligation(s) as set forth in Rule 13.1 of part 1 of this rulebook has been previously satisfied by its Principal, each Affiliate is responsible for the liabilities and obligations arising out of, or in connection with, its Maestro programs, irrespective of any (i) action taken by it to satisfy such liability or obligation with the Principal or (ii) agreements between the Principal and Affiliate.

Additional Regional Information

Asia/Pacific Geographical Region

Refer to Appendix A, "Geographical Regions," in part 2 of this rulebook.

Technical Specifications

Refer to Appendix B, "Technical Specifications," in part 2 of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
1.1 Types of Customers	A
1.6.7 Additional Rules for Participation	A
1.7 Termination of License	A
4.2 Protection and Registration of the Marks	B
4.5 Display on Cards	B
6.4 PIN and Signature Requirements	A
6.13 Issuer Responsibilities to Cardholders	B
7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only	A
7.9 POS Terminal and Terminal Requirements	A
7.11 Additional Requirements for POS Terminals	A
7.17 Connection to the Interchange System	A
7.18 Card Capture	A
7.23 ATM Access Fees	B
7.24 Return Merchandise Adjustments, Credits, and Other Specific Terms of a Transaction	B
9.2 POS Transaction Types	B
9.8 Authorizations	A

Chapter 16 Canada Region

This chapter contains Rule variations or additional Rules applicable only to the Canada Region.

Overview

Set forth below are the Rule variations to the *Maestro Global Rules* and additional Rules for the Canada Region. In most cases, the Canada chapter supplements part 1 of this rulebook and Canada Customers must comply with the Rules in both part 1 and Chapter 16, "Canada Region," of this rulebook.

If a subsection in the Canada regional chapter contains the full set of Rules applicable to Canada Customers, in place of the corresponding chapter in part 1 of this rulebook, then this is clearly mentioned, and Canada Customers are required to comply only with the Rules in that Canada chapter.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

4.5 Display on Cards

NOTE

Additional Rules on this topic appear in Section 16a, "Canada Region Code of Conduct Related Rules," of this rulebook.

6.4 PIN and Signature Requirements

6.4.1 PIN Issuance

The following replaces the second paragraph of Chapter 6, "Issuing," Rule 6.4.1 in part 1 of this rulebook:

The PIN may be from four (4) to twelve (12) alphanumeric characters.

6.10 Selective Authorization

NOTE

Additional Rules on this topic appear in Section 16a, "Canada Region Code of Conduct Related Rules," of this rulebook.

6.13 Issuer Responsibilities to Cardholders

NOTE

Additional Rules on this topic appear in Section 16a, "Canada Region Code of Conduct Related Rules," of this rulebook.

6.17 Additional Rules for Issuing

NOTE

Additional Rules on this topic appear in Section 16a, "Canada Region Code of Conduct Related Rules," of this rulebook.

7.1 Acquirer Obligations and Activities

7.1.1 Signing a Merchant—POS and Electronic Commerce Only

NOTE

Additional Rules on this topic appear in Section 16a, "Canada Region Code of Conduct Related Rules," of this rulebook.

7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only

7.2.1 Merchant Surcharging

NOTE

Additional Rules on this topic appear in Section 16a, "Canada Region Code of Conduct Related Rules," of this rulebook.

7.9 POS Terminal and Terminal Requirements

7.9.3 PIN Entry Device

The following replaces Chapter 7, "Acquiring," Rule 7.9.3 (3). in part 1 of this rulebook:

3. be capable of allowing entry of PINs having from four (4) to twelve (12) characters.

7.10 Hybrid POS Terminal and Hybrid Terminal Requirements

7.10.1 Chip Liability Shift

Effective 31 December 2015, the liability for Canada intraregional counterfeit Transactions in which one Customer (either the Issuer or the Acquirer) is not yet EMV-compliant will be borne by the non–EMV-compliant party in the Transaction process. The chip liability shift is implemented in chargeback reason code 70.

7.12 Additional Requirements for ATMs

The following replaces Chapter 7, "Acquiring," Rule 7.12 (2) in part 1 of this rulebook:

2. assign letter-number combinations as described in Rule 7.12 in part 1 of this rulebook.

7.15 Requirements for Transaction Receipts

7.15.6 PAN Truncation Requirements

7.15.6.2 Terminals

The following replaces Chapter 7, "Acquiring," Rule 7.15.6.2, in part 1 of this rulebook:

One (1) of the following options must be used:

1. print the PAN on the receipt but truncate a minimum of any four (4) digits of the PAN. The Corporation strongly recommends that all truncated digits be replaced with fill characters that are neither blank spaces nor numeric characters, such as "x", "*", or "#", or
2. print the PAN on the receipt but render a minimum of any four (4) digits of the PAN indeterminable by any Corporation approved method.

The Corporation 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 "#".

7.17 Connection to the Interchange System

In addition to the rules in Chapter 7, "Acquiring," Rule 7.17 in part 1 of this rulebook, the following applies:

Customers that acquire Transactions must make available for connection to the Interchange System at least seventy-five percent (75%) of the online ATMs established by that entity (including its parents, subsidiaries and affiliates) in each major metropolitan area in which at least 10,000 of such entity's debit Cardholders reside.

The Census Metropolitan Area (CMA) as defined by the Canadian government will be used as the measure.

7.23 ATM Access Fees

7.23.1 Domestic Transactions

The following replace Chapter 7, "Acquiring," Rule 7.23, paragraph 1 in part 1 of this rulebook:

Upon complying with the ATM Access Fee notification requirements of the Rules, Acquirers in the Canada Region may assess an ATM Access Fee on a Transaction initiated with a Card that was issued in the Canada Region so long as the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory fashion.

7.23.1.1 Transaction Field Specifications

At the time of each Transaction on which an ATM Access Fee is imposed, the Acquirer of such Transaction must transmit the amount of the ATM Access Fee in the field specified in the *Single Message System Specifications* manual.

7.23.1.2 Non-Discrimination Regarding ATM Access Fees

An Acquirer must not charge an ATM Access Fee in connection with a Transaction that is greater than the amount of any ATM access fee charged by that Acquirer in connection with the transactions of any other network accepted at that Terminal.

7.23.1.3 Notification of ATM Access Fee

An Acquirer that plans to add an ATM Access Fee must notify its Sponsoring Principal, in writing, of its intent to do so prior to the planned first imposition of such ATM Access Fee by the Acquirer.

The Principal must update the Location Administration Tool (LAT) regarding its or its Affiliates' imposition of ATM Access Fees.

7.23.1.4 Cancellation of Transaction

Any Acquirer that plans to add an ATM Access Fee must notify the Cardholder with a screen display that states the ATM Access Fee policy and provides the Cardholder with an option to cancel the requested Transaction.

7.23.1.5 Terminal Signage, Screen Display, and Transaction Record Requirements

An Acquirer that plans to add an ATM Access Fee to a Transaction must submit proposed Terminal screen display and receipt copy that meets the requirements of the Rules to its Sponsoring Principal, in writing, for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook).

In addition, if the Acquirer displays Terminal signage, the Acquirer must submit proposed Terminal signage copy that meets the requirements of the Rules to its Sponsoring Principal, in writing, for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook).

The Sponsoring Principal has the right to determine the acceptability of any new, or changes to previously-approved, Terminal signage, screen display, and receipt copy. In cases of conflict between the Acquirer and its Sponsoring Principal Customer, the Corporation has the sole right to determine the acceptability of any and all Terminal signage, screen display, and receipt copy.

7.23.1.5.1 Additional Requirements for Terminal Signage

An Acquirer that plans to add an ATM Access Fee to a Transaction may optionally display signage that is clearly visible to Cardholders on or near all Terminals at which ATM Access Fees apply.

The minimum requirement for ATM Access Fee Terminal signage text is wording that clearly states:

1. the name of the ATM Owner and Principal;
2. that the Transaction may be subject to an ATM Access Fee that will be deducted from the Cardholder's Account in addition to any Issuer fees;
3. the amount of, calculation method of, or Corporation-approved generic signage regarding the ATM Access Fee;
4. that the ATM Access Fee is assessed by the Acquirer instead of the Issuer; and
5. that the ATM Access Fee is assessed on Canada Cardholders only

The minimum requirements for Terminal signage (physical characteristics) are as follows:

1. the signage must bear the heading "Fee Notice";
2. the size of the Terminal signage must be a minimum of four (4) inches in height by four (4) inches in width;
3. the text must be clearly visible to all. It is recommended that the text be a minimum of fourteen (14) point type;
4. the heading must be clearly visible to all. It is recommended that the text be a minimum of eighteen (18) point type.

A model for Terminal signage regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.1.5.2 Additional Requirements for Terminal Screen Display

An Acquirer that plans to add an ATM Access Fee to a Transaction must present a screen display message that is clearly visible to Cardholders on all Terminals at which ATM Access Fees apply. If the Cardholder is given the option of choosing a preferred language in which to conduct the Transaction, the screen display message concerning ATM Access Fees must be presented to the Cardholder in that chosen language.

If an Acquirer displays the Corporation-approved generic ATM Access Fee signage, the Acquirer must include the amount of the ATM Access Fee as part of the Terminal screen display.

A model for the Terminal screen display regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.1.5.3 Additional Requirements for Transaction Records

An Acquirer that adds an ATM Access Fee to a Transaction must make available to the Cardholder on its Terminal receipt the ATM Access Fee information required by this Rule 7.23.1.5.3, in addition to any other information the Acquirer elects or is required to provide.

The minimum requirements for the Terminal receipt are:

1. a statement of the amount disbursed to the Cardholder;
2. a statement of the ATM Access Fee amount with language clearly indicating it is a fee imposed by the Acquirer;
3. a separate statement of the combined amount of the ATM Access Fee and the disbursed amount, with language clearly indicating that this amount will be deducted from the Cardholder's Account.

A model for Terminal receipt text regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

9.3 Terminal Transaction Types

9.3.1 Issuer Requirements

In addition to the requirements of Chapter 9, "Processing Requirements," Rule 9.3.1 in part 1 of this rulebook, the following applies:

Issuers must offer to each Cardbase that offers access to an Account, as applicable, the following Transactions:

1. cash withdrawal from a savings Account;
2. cash withdrawal from a checking (or chequing) Account.

9.3.2 Acquirer Requirements

In addition to the requirements of Chapter 9, "Processing Requirements," Rule 9.3.2 in part 1 of this rulebook, the following apply:

Terminals must offer the following Transactions to the extent permitted by law, regulation, or both.

1. cash withdrawal from a savings Account;
2. cash withdrawal from a checking (or chequing) Account;
3. 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).

1. balance inquiry—checking (or chequing) Account;
2. balance inquiry—savings Account;
3. balance inquiry—credit card;
4. transfer from checking (or chequing) to savings Account;
5. 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.

9.3.2.1 Acquirer Optional Transactions

In addition to the requirements of Chapter 9, "Processing Requirements," Rule 9.3.2.1 in part 1 of this rulebook, the following applies:

Terminals may offer a cash withdrawal from no Account specified to the extent permitted by law, regulations, or both.

9.8 Authorizations

9.8.2 Terminal Transaction Routing

In addition to the requirements of Chapter 9, "Processing Requirements," Rule 9.8.2 in part 1 of this rulebook, the following applies:

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 Mark:

1. the resulting Transaction must be routed to the Interchange System; or
2. the Issuer receiving such Transaction must:
   a. report such Transaction in accordance with the schedule and pay a Brand Fee for such Transaction as required

except when the Transaction was:

1. processed between a Principal (or its processor) and one of its Affiliates (or its processor), or
2. processed between two Affiliates (or their processors) sponsored into the Corporation by the same Principal.

NOTE

The first paragraph of this subsection does not apply if the transaction is a proprietary transaction.

10.2 Settlement

In addition to the rules in Chapter 10, "Settlement and Reconciliation," Rule 10.2 in part 1 of this rulebook, the following applies:

All domestic Transactions must be settled in Canadian dollars (CAD), and Customers must submit a Net Settlement Information Form (NSIF) to participate in the MasterCard Intracurrency Settlement Service.

Additional Regional Information

Canada Geographical Region

For further information refer to Appendix A, "Geographical Regions," in part 2 of this rulebook.

Technical Specifications

Refer to Appendix B, "Technical Specifications," in part 2 of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
6.4 PIN and Signature Requirements	A
7.9 POS Terminal and Terminal Requirements	A
7.10.1 Chip Liability Shift	A
7.12 Additional Requirements for ATMs	A
7.15 Requirements for Transaction Receipts	B
7.17 Connection to the Interchange System	A
7.23 ATM Access Fees	B
9.3 Terminal Transaction Types	A
9.8 Authorizations	A

Section 16a—Canada Region Code of Conduct Related Rules

This section contains Rule variations or additional Rules applicable only to the Canada Region, with regard to the Code of Conduct.

Overview

Set forth below are the Rule variations to the *Maestro Global Rules* and additional rules for the Canada Region. In most cases, the Canada chapters supplement part 1 of this rulebook and Canada Customers must comply with the rules in both part 1 and Chapter 16, "Canada Region," of this rulebook.

If a subsection in this Canada regional chapter contains the full set of Rules applicable to Canada Customers, in place of the corresponding chapter in part 1 of this rulebook, then this is clearly mentioned, and Canada Customers are required to comply only with the rules in this Canada chapter.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

Definitions

Solely for the purposes in this Section 16a, the following terms have the meaning set forth below:

Card

A card issued by a Customer enhanced with the Mark(s), pursuant to License and in accordance with the Standards, that provides access to eligible Accounts. Unless otherwise stated herein, any reference to Card does not encompass an Access Device or a Mobile Payment Device.

Cardholder

The authorized user of a Card.

Premium Card

Maestro branded Cards that are issued in the Canada Region by a Canada Customer to a well-defined class of Cardholders in accordance with the Corporation's requirements and specifications for same.

Transaction

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

4.5 Display on Cards

In addition to the Rules in Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook, the following applies:

When the Marks appear on a Card containing other local/regional POS debit marks and/or local/international ATM marks, no other local/regional POS debit mark and/or local/international ATM mark, symbol or logo may be, or appear to be, larger or more important than the Marks. To maintain visual parity, the Marks must be at least as prominent as other local/regional POS debit marks and/or local/international ATM marks on the Card and must be at least the same size and the same color treatment as any other local/regional POS debit mark and/or local/international ATM mark on the Card. When other local/regional POS debit marks and/or local/international ATM marks appear on a Card, those marks must appear on the same side of the Card as the Marks.

6.10 Selective Authorization

In addition to the Rules in Chapter 6, "Issuing," Rule 6.10 in part 1 of this rulebook, the following applies:

For the purpose of effecting a Transaction, an Issuer must not place competing domestic applications of other POS debit networks on a Card. An Issuer may place complementary domestic applications on a Card.

6.13 Issuer Responsibilities to Cardholders

In addition to the rules in Chapter 6, "Issuing," Rule 6.13 in part 1 of this rulebook, the following applies:

Premium Cards may only be provided to a well-defined class of Cardholders, based on individual spending and/or income thresholds. An Issuer may only provide a Premium Card to a person that has applied for or consented to receiving a Premium Card.

6.17 Additional Rules for Issuing

When an Issuer in Canada issues a Card that contains the Marks and any other POS debit mark, the Issuer must not prioritize Maestro on the Financial Institution Table (FIT).

7.1 Acquirer Obligations and Activities

7.1.1 Signing a Merchant—POS and Electronic Commerce Only

7.1.1.4 Information to Merchants

In addition to the rules in Chapter 7, "Acquiring," Rule 7.1.1 in part 1 of this rulebook, the following applies:

Acquirers must provide a minimum of ninety (90) days notice to Merchants of any fee increases, or the introduction of a new fee related to any Card or Transaction. A Merchant may opt out of its merchant agreement, without penalty by the Acquirer, within ninety (90) days of receiving notice of the fee increase or introduction of a new fee. A Merchant may not opt out of the merchant agreement if the fee increase is made in accordance with a pre-determined fee schedule, provided such fee schedule is included in the merchant agreement.

An Acquirer must obtain the Merchant's express consent each time a Card with new Marks, or a Card with Marks not previously accepted by the Merchant, will be accepted by the Merchant.

Acquirers must provide monthly statements to Merchants that include a sufficient level of detail and are easily understood. Merchant statements must include:

1. The discount rate for each Card associated with a unique interchange program;
2. Interchange rates, and if applicable, all other rates charged to the Merchant by the Acquirer;
3. The number and volume of Transactions associated with a unique interchange program;
4. The total amount of fees applicable to each rate; and
5. Details of each fee that relate to the Corporation.

7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only

7.2.1 Merchant Surcharging

In addition to the rules in Chapter 7 "Acquiring," Rule 7.2.1 in part 1 of this rulebook, the following applies:

In addition to a discount for cash, a Merchant may provide a discount to its customers for other forms of payment, including differential discounts for other payment brands. Such discounts must be clearly communicated at the point of interaction.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
4.5 Display on Cards	B
6.10 Selective Authorization	B
6.13 Issuer Responsibilities to Cardholders	A
6.17 Additional Rules for Issuing	A
7.1 Acquirer Obligations and Activities	A
7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only	A

Chapter 17 Europe Region

This chapter contains Rule variations and additional Rules for the Europe Region.

Overview

Set forth below are the Rule variations to the *Maestro Global Rules* and additional Rule for the Europe Region. In most cases, the Europe chapter supplements part 1 of this rulebook and Europe Customers must comply with the Rules in both part 1 and Chapter 17, "Europe Region," of this rulebook.

If a section in the Europe regional chapter contains the full set of Rule applicable to Europe Customers, in place of the corresponding Rule in part 1 of this rulebook, then this is clearly mentioned, and Europe Customers are required to comply only with the Rule in that Europe section.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

Definitions

In addition to the defined terms in the "Definitions" chapter in part 1 of this rulebook, the following apply:

Account

In the EEA, Account means any type of account (i.e. credit, debit, etc).

Address Verification Service (AVS)

A process whereby the Issuer checks the address given for a Mail Order/Telephone Order (MO/TO) Transaction.

Cardholder Authority

A Cardholder's instructions requesting a Merchant to perform a non-face-to-face purchase Transaction.

Card Verification Code (CVC) 2

A Card Verification Code that must be indent printed in a white panel adjacent to the signature panel that can be used to help identify counterfeit cards.

Commercial Card

In the EEA, a Card issued to an undertaking or public sector entity or one of its employees and that is intended for use in connection with business expenses made by that undertaking or public sector entity or by its employee, or a Card issued to a self-employed natural person engaged in a business activity and that is intended for use for business expenses. Cards fitting the above definition that are in issuance in the EEA after 31 December 2010 must be identifiable as Commercial Cards.

Consumer Card

In the EEA, a Card issued to a natural person that is not used primarily for business expenses.

Credit Card

In the EEA, a Consumer Card that allows the Cardholder to make purchases with a certain credit amount, which can be settled in full by the end of a specified period (which typically is interest-free) or can be settled in part, with the remaining balance being taken as credit and charged with interest. A Credit Card may be linked to a current account at a deposit-taking institution or to an account that has been set up specifically for the use of the Credit Card. Credit Cards include charge (or delayed debit) Cards. A charge (or delayed debit) Card is a Card that allows the Cardholder to make purchases but does not offer credit, the amount of the debit having to be settled in full only after a specified period (which typically is interest-free). A charge (or delayed debit) Card may be linked to a current account at a deposit-taking institution or to an account that has been set up specifically for the use of then charge (or delayed debit) Card.

CVC 2/AVS Check

Automated verification by the Issuer of CVC 2 and address details provided for a Mail Order/Telephone Order (MO/TO) Transaction. For Intracountry Transactions in Ireland with a Transaction date prior to 1 January 2012, Issuer verification of the CVC 2 is not mandated.

Debit Card

In the European Economic Area (EEA), a card that allows a cardholder to charge purchases directly to a current account at a deposit-taking institution. The debit card serves as a device to access funds stored in a current account. A debit card transaction is always directly charged to a current account i.e. no later than two business days after the clearing of the transaction, whereas a credit (or charge or delayed debit) card transaction may be settled by the end of a specified period or charged to a current account more than two business days after the clearing of that transaction.

European Economic Area (EEA)

The following countries and their related territories : Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

Intracountry Transaction

A Transaction acquired at a POI Terminal located in the same country in which the Card is issued. A Transaction qualifies as an Intracountry Transaction when it is completed using a Card that bears the Marks either alone or in combination with the marks of another eligible payment scheme, and it is processed as a Transaction, as shown by the Card product identification in the Transaction record, via either the Interchange System or a different network.

Intra-SEPA Transaction

A Transaction completed using a Card issued in a country covered by Section 17b at a POI Terminal located in a country covered by Section 17b.

Maestro *PayPass*

Maestro® *PayPass*™ is a contactless payment functionality that uses radio frequency ("RF") technology to exchange Transaction data between a Chip Card and a RF-enabled POS Terminal that bears the Maestro *PayPass* logo.

Mail Order Transaction

A non-face-to-face POS Transaction where the Cardholder provides a written Cardholder authority.

SEPA Cards Framework (SCF)

The SEPA Cards Framework as published by the European Payments Council, as it may be amended from time to time.

Service Fee

Fee paid by the issuer to the acquirer for the service provided in relation to an ATM or PIN-based in-branch Transaction.

Telephone Order Transaction

A non–face-to-face POS Transaction where the Cardholder provides a Cardholder authority through the telephone system.

UK SFD Regulations

The UK Financial Markets and Insolvency (Settlement Finality) Regulations 1999.

Volume

The financial value of a group of Transactions, as opposed to the number of Transactions.

NOTE

Additional Rules on this topic appear in Section 17b, "Single European Payment Area Rules," of this rulebook.

1.1 Types of Customers

The following Rules replace paragraph 1 of Rule 1.1 in part 1 of this rulebook:

In the Europe Region a Customer may be both an Affiliate and a Principal.

1.7 Termination of License

In addition to the Rules in Chapter 1, "Participation," Rule 1.7 in part 1 of this rulebook, the following apply:

All publicity about the withdrawal/termination must be approved or issued by MasterCard Europe.

Customers must continue to fulfill their obligations with regard to confidentiality. Customers must immediately, in accordance with the instructions of the Corporation and under the supervision of the Corporation, either destroy or deliver to the Corporation all confidential and/or proprietary systems and documentation previously received as a Customer.

In addition, Customers must ensure the safekeeping or, at their option, destruction of any materials or equipment which could be used to continue to generate Transactions.

If a Customer decides to destroy any items, this destruction must be carried out under the supervision of the Corporation and a detailed certificate itemizing what has been destroyed must be produced and signed jointly by the Customer and the Corporation.

2.2 License Application

In addition to the Rules in Chapter 2, "Licensing and Licensed Activities," Rule 2.2 in part 1 of this rulebook, the following apply:

The License covers both issuing and acquiring unless otherwise stated.

2.2.1 Single European Payment Area License

NOTE

Rules on this topic appear in Section 17b, "Single European Payments Area Rules," of this rulebook.

2.3 Area of Use

In addition to the Rules in Chapter 2, "Licensing and Licensed Activities," Rule 2.3 in part 1 of this rulebook, the following apply:

1. If the Customer has several Licenses, each may define a different Area of Use;
2. Customers are not required to have a physical establishment in the Area of Use.
3. An Issuer must use an ICA for Card issuance that accurately reflects the Area of Use in the corresponding License. An Issuer must use a BIN or BIN range for Card issuance that accurately reflects the Area of Use in the corresponding License. Different ranges within a BIN may be linked to ICAs assigned for different Areas of Use.

2.3.1 Transaction Location

The following additional Rules apply in the Europe Region.

2.3.1.1 Face-to-Face Transactions (including Cardholder Activated Terminals)

The Transaction takes place at the location where the Cardholder is present and uses the Card to effect payment to the Merchant or to receive a cash advance.

2.3.1.3 Remote Transactions (for example, Electronic Commerce)

The Transaction takes place in the country where the Merchant is established and organizes the fulfillment of orders and the generation of Transactions for entry into the system.

2.3.3 Central Acquiring

The Rules in this section apply in the Europe Region in place of Rule 2.3.3, paragraphs 3, 4, and 5.

Provided that they comply with the provisions of this Rule 2.3.3, Customers that hold a License may centrally acquire Transactions (both POS and electronic commerce) from Merchants as described in Rule 2.3.3.4 below, including those undertaken in countries for which the Customer does not hold a License. Customers must not acquire Transactions from Merchants situated outside their Area of Use, except pursuant to this Rule 2.3.3.

This Rule 2.3.3 applies to central acquiring in the Region by Customers that hold a License for any country in the Region.

2.3.3.1 Central Acquiring Registration

Customers must have completed the central acquiring registration process before they centrally acquire. The central acquiring registration letter specifies the countries in which a Customer may centrally acquire intra-European POS and electronic commerce Transactions.

In order to be registered for central acquiring, the Customer must meet the central Acquirer criteria set forth in Rule 2.3.3.2 below.

2.3.3.2 Central Acquirer Service Requirements

The Customer must authorize, clear, and settle centrally acquired Transactions in a manner that does not disadvantage the Cardholder, the Merchant, or the Issuer involved in the Transaction in comparison with non-centrally acquired Transactions. The Customer must also comply with the requirements defined below.

1. Authorizations

   Central Acquirers must provide Issuers with all information required in the authorization request, as set forth in the *Customer Interface Specification* manual.

2. Clearing

   Central Acquirers must provide details in the clearing record of the location, city, and country where the Transaction took place.

For specific Merchant sectors, central Acquirers must provide additional information in the clearing record if required by the Europe Region, using the message formats detailed in the *IPM Clearing Formats* manual.

2.3.3.3 Intracountry Rules

Central Acquirers must comply with the intracountry rules of a country in which they centrally acquire Transactions.

The Corporation will provide central Acquirers, on request and upon payment of the corresponding fee, with the intracountry rules of the country or countries covered by the request.

2.3.3.4 Centrally Acquired Merchants

An Acquirer may centrally acquire Transactions from **any Merchant** located in any one of the following **Western or Central European countries**: Andorra, Austria, Belgium, Bulgaria, Channel Islands, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Isle of Man, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, Vatican City.

In all other Europe Region countries, an Acquirer may only centrally acquire Transactions of a Merchant that:

1. operates in more than two countries in the Region either directly; or through wholly-owned subsidiaries; or through a joint venture that requires consolidation on the balance sheet of the central company; or under the same brand name through franchise and/or management contracts.
2. operates a centrally managed delivery system that services subsidiaries and local operators and is used to process orders, reservations, sales or payments; supports the delivery of services (for example, tickets/contracts) or goods; and manages stock or service availability.
3. operates a centrally managed accounting system that monitors treasury and cash management and payment collections and is used to channel and support payment system authorizations.

2.3.3.4.1 Updating of Merchant Details

To ensure correct system implementation and Transaction monitoring, central Acquirers must inform the Corporation of any changes to the Merchant details of any Merchant (excluding Merchants in Western and Central European countries) where Transactions are centralized, including changes to the Merchant's name and address and to the MCC used for centrally acquired Transactions. The changes must be communicated to the Corporation by submitting a central acquiring application form that contains the new details. If changes to Merchant details are not communicated to the Corporation within thirty (30) business days of receipt of a warning letter, noncompliance assessments may be applied.

2.3.3.5 Registration Procedure

To register to centrally acquire in the **Western and Central European countries** listed in Rule 2.3.2.4 above, the Customer must submit to the Corporation a single application form covering all such Western and Central European countries. The central acquiring registration letter will cover all Western and Central European countries.

To register to centrally acquire in other countries in the Region, the Customer must submit to the Corporation an application form for each Merchant and country where the Customer wishes to centrally acquire Transactions.

2.3.3.6 Extension of Registration

In the **Western and Central European countries** listed in Rule 2.3.3.4 above, a central Acquirer is not required to comply with any formal procedures in order to extend its central acquiring Activities to a new Merchant or country in Western and Central Europe.

In **all other countries in the Region**, a Customer that wishes to extend its central acquiring Activities to a new Merchant or country must follow the registration procedure set forth in Rule 2.3.2.5 above.

2.3.3.7 Interchange Fee Requirements

If a central Acquirer acquires an Intracountry Transaction, the following principles apply to the interchange fee:

1. the central Acquirer may agree upon bilateral interchange fees with the Issuer;
2. if no bilateral interchange fees have been agreed, the intracountry fallback interchange fees, as defined in the intracountry rules of the country in which the Transaction took place, apply;
3. if at the time of the Transaction no intracountry fallback interchange fees exist in the country where the Transaction took place, the intra-European fallback interchange fees apply.

If a central Acquirer acquires a Non-Intracountry Transaction, the following principles apply to the interchange fee:

1. the central Acquirer may agree upon bilateral interchange fees with the Issuer;
2. if no bilateral interchange fees have been agreed and the Transaction took place with a Card issued in the Region, the intra-European fallback interchange fees apply.

2.3.3.8 Settlement of Disputes

Any disputes relating to central acquiring will be resolved by the Corporation in accordance with the Standards.

2.3.3.9 Noncompliance

The following are examples of violations of the central acquiring rules for which noncompliance assessments may be applied:

1. Engaging in central acquiring without first registering,
2. Engaging in central acquiring in non-notified countries or of non-notified Merchants (not applicable for Western and Central European countries).
3. Failure to comply with intracountry rules (including application of incorrect interchange fees) resulting in financial loss to another party.
4. Incorrect data in Interchange System messages (including incorrect country code) resulting in financial loss to another party.

3.1 Standards

Transactions undertaken in Europe with Cards issued by European Customers are considered intra-European Transactions.

The intra-European Maestro Rules, including interchange fees, apply to intra-European Transactions.

The Rules in this Europe chapter allow access to PIN-Based In-Branch Terminals in bank branches for all Cards. This service is not available for MasterCard cards that do not display the Marks. Such service involves the manual intervention of a bank clerk, while ATMs, indoors or outdoors, do not. Issuers must support the PIN-Based In-Branch service; for Acquirers, it is optional.

3.1.3 Rules Applicable to Intracountry Transactions

The following are additional Rules applicable to intracountry Transactions. Refer to Rule 10.8 in Part 1 of this rulebook regarding the establishment of intracountry interchange fees and intracountry service fees.

The following two options apply as regards establishment of the rules to be applied to Intracountry Transactions. Customers may change from one option to another upon notice in writing to MasterCard Europe, and fulfillment of any requirements associated with the new option.

Maestro Global Rules (the Rules)

Customers may apply the Rules (including Europe Region Rules) to Intracountry Transactions. If one of the other options does not apply, then this option applies by default.

Intracountry Fallback Rules (75 percent Rule)

If permitted by local law, Customers holding Licenses for the country (including SEPA Licenses) and representing, during the year preceding the agreement, at least 75 percent of each of the Maestro issuing and acquiring intracountry Volumes (excluding on-us Volumes), have the power to agree on fallback rules applicable to all Intracountry Transactions, including those acquired by Customers outside the country. Intracountry fallback rules must be agreed by a least two Issuers and at least two Acquirers Licensed to engage in Activity in the country.

The percentage is calculated separately for each Card product, as determined by the Card product identifier, and functionality (POS vs. ATM).

Intracountry fallback rules remain in effect until changed or challenged. If intracountry fallback rules are challenged because the Customers agreeing to them no longer meet the 75 percent threshold, the Rules (including the Europe Region Rules) will apply in their place, as from the date when MasterCard Europe has determined that the 75 percent threshold is no longer met.

Intracountry fallback rules must be non-discriminatory, justifiable, and not in conflict with the Rules (including the Europe Region Rules). Intracountry fallback rules must not discriminate against Cardholders (including international Cardholders) or jeopardize the integrity and consistency of the payment scheme.

3.1.3.1 Order of Precedence

For any Intracountry Transaction, the intracountry Rules established by the Corporation apply, or if none, the intracountry fallback Rules established by Customers pursuant to the preceding Rule apply, or if none, the intraregional Rules apply, or if none, the interregional Rules apply.

3.1.4 Communication of Intracountry Fallback Rules

Customers that agree to intracountry fallback rules must provide MasterCard Europe with a copy of the intracountry fallback rules as well as with any subsequent changes to those rules. The Corporation must be notified of intracountry fallback rules well in advance of their effective dates, unless 4 exceptional circumstances make this impossible. Exceptional circumstances must be related to events beyond the control of the Customers, such as changes in laws or regulations, compliance with which requires immediate action.

Intracountry fallback rules that have not been notified to and acknowledged by MasterCard Europe are not applicable.

MasterCard Europe will endeavor to publish intracountry fallback rules and their revisions at least three calendar months prior to their effective date. If exceptional circumstances apply, the period will be not less than one calendar month before the effective date. If necessary, the initially notified effective date will be delayed to respect these timeframes.

3.3 Choice of Laws

The following Rules apply in the Europe Region in place of the global rules:

Licenses are governed by and construed according to the applicable law mentioned in the particular License, without reference to conflict-of-laws or similar provisions that would mandate or permit the application of the substantive law of any other jurisdiction.

The courts mentioned in the particular License have exclusive jurisdiction for the resolution of any dispute relating to rights and obligations deriving from Licenses.

Licenses concluded after 1 January 2007 specify English law and courts.

The Rules are governed by and construed according to English law, without reference to conflict-of-laws or similar provisions that would mandate or permit the application of the substantive law of any other jurisdiction. English courts have exclusive jurisdiction for the resolution of any dispute relating to the Rules between two Customers holding Licenses for countries in the Europe Region.

3.4 Examination and Audits

The following additional Rules apply in the Europe Region.

3.4.1 Operational Audits

MasterCard Europe may conduct audits of a European Customer's or its Service Provider's Activities if it has reasonable grounds to believe that the Rules are being violated or that the Customer poses a significant risk to the Corporation.

All out-of-pocket expenses incurred by MasterCard Europe in connection with such an audit must be paid by the Customer if the audit determines that the Customer or its Service Provider has violated the Rules.

3.4.2 Financial Audits

If MasterCard Europe has reason to believe that the financial accounts produced by a Customer do not correctly portray the Customer's financial situation, MasterCard Europe may require the Customer to be audited by independent accountants chosen by MasterCard Europe. The standards and scope of the audit will be decided by MasterCard Europe. All out-of-pocket expenses incurred by MasterCard Europe in connection with such an audit must be paid by the Customer if the audit determines that the financial accounts do not correctly portray the Customer's financial situation.

3.4.3 Customer's Duty to Provide Information

Any Customer subject to an audit must provide all information requested by MasterCard Europe in connection with the audit. If a Service Provider is also being audited, the Customer who uses the Service Provider must ensure that the Service Provider provides the requested information.

3.6 Non-discrimination

NOTE

Additional Rules on this topic appear in Section 17b, "Single European Payment Area Rules," of this rulebook.

3.6.2 Terminal Transactions

In addition to the Rules in Chapter 3, "Customer Obligations," Rule 3.6.2 in part 1 of this rulebook, the following applies:

Acquirers must not discriminate against any Card, with regard to processing Transactions, including Cards issued by other Customers within the same country.

Issuers must not discriminate against any Terminal with regard to processing and authorizing Transactions, including Terminals owned by other Customers within the same country.

3.7 Provision and Use of Information

In addition to the Rules in Chapter 3, "Customer Obligations," Rule 3.7 in part 1 of this rulebook, the following apply:

A Customer must only use confidential information in connection with its Program.

If a Customer is required to disclose confidential information due to law, regulation or a court order, the Customer must seek to ensure that the recipient keeps the information confidential. The Customer must inform MasterCard Europe immediately if it receives such a request.

3.8 Record Retention

In addition to the Rules in Chapter 3, "Customer Obligations," Rule 3.8 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.

3.21 Additional Obligations

In addition to the Rules in Chapter 3, "Customer Obligations," Rule 3.21 in part 1 of this rulebook, the following apply:

1. Within nine (9) months from the date of their License being granted, Customers must:

   a. issue Cards; and/or

   b. acquire Transactions.

2. Customers must make every effort to issue the agreed number of Cards and to acquire the agreed number of Merchants and to open the agreed number of ATMs, PIN-Based In-Branch Terminals, or both as specified in their business plan and agreed with MasterCard.

3. Customers must provide facilities to handle queries and disputes on Transactions. This may involve the Acquirer requesting documentation or evidence from the Merchant, the ATM or the PIN-Based In-Branch Terminal on behalf of the Issuer. Customers must advise the Corporation of the entity responsible for processing chargebacks on their behalf.

3.22 Data Protection

In addition to the defined terms in the "Definitions" chapter in part 1 of this rulebook, the following apply solely to Rule 3.22:

3.22.1 Definitions

Solely for the purposes of this Rule 3.22,

1. "Controller" shall mean the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.
2. "Data Subject" shall mean a Cardholder, or Merchant, or other natural or legal person (to the extent a legal person is subject to national data protection law) who's Personal Data are processed by a Customer in the EEA or Switzerland and the Corporation.
3. "EU Privacy Directive" shall mean, collectively, the 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 and Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as may be amended from time to time.
4. "Personal Data" shall mean any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity.
5. "Processor" shall mean the entity which processes Personal Data on behalf of a Controller.
6. "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, Corporation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction of such data.
7. "Transaction-related Personal Data" shall mean the Personal Data required for authorizing, recording, settling and clearing a Transaction processed by the Interchange System.

3.22.2 Processing of Transaction-Related Personal Data

With regard to Transaction-related Personal Data, Customers in the EEA and Switzerland must comply with the applicable national legislation implementing the EU Privacy Directive or any other applicable data protection law. Customers are Controllers with regard to the Processing of Personal Data for the purposes of authorizing, recording, clearing and settling Transactions, and the Corporation is a Processor for these purposes.

The Corporation will, to the extent it acts as a Processor, only undertake Processing of Personal Data in accordance with the Standards and will comply with security obligations equivalent to those imposed on the Customers as Controllers by Article 17 of the EU Privacy Directive 95/46, as implemented by national legislation.

3.22.3 Data Subject Notice and Consent

Customers in the EEA or Switzerland must ensure that the Data Subjects are properly informed and, if necessary, have given proper consent in accordance with applicable laws and regulations, that Personal Data relating to them may be used, disclosed, or otherwise processed by the applicable Customer and the Corporation as set forth in Rule 3.7.1 in Part 1 of this rulebook.

In accordance with applicable law, Customers in the EEA or Switzerland must ensure that Data Subjects are properly informed, at a minimum:

1. that Data Subjects have the right to (a) request access to and receive information about the Personal Data maintained by the applicable Customers or the Corporation, (b) update and correct inaccuracies in the Personal Data and (c) have the Personal Data blocked or deleted as appropriate:
2. that Data Subjects may withdraw any consent they previously provided to the applicable Customer or the Corporation or object at any time on legitimate grounds to the Processing of Personal Data;
3. about the choices and means that Data Subjects have for limiting the Processing of Personal Data by the Corporation;
4. that Personal Data may be processed outside the EEA or Switzerland; and
5. about the categories of recipients of Personal Data.

3.22.4 Data Subject Access to Personal Data

In accordance with applicable law, Customers in the EEA or Switzerland must develop and implement appropriate procedures for handling requests by Data Subjects for access to, correction and/or deletion of Personal Data maintained by the applicable Customer or the Corporation. The Corporation will cooperate fully with Customers in responding to such requests and will provide access to Personal Data maintained by the Corporation. Customers must cooperate with the Corporation to assist Customers in complying with requests for access to such Personal Data.

If an access request is made directly to the Corporation, Customers must cooperate with the Corporation in promptly responding to the request.

3.22.5 Integrity of Personal Data

Each Customer in the EEA or Switzerland must take reasonable steps to ensure that the Personal Data the Customer provides to the Corporation are reliable for their intended use and are accurate, complete, and current.

4.2 Protection and Registration of the Marks

In addition to the Rules in Chapter 4, "Marks," Rule 4.2 in part 1 of this rulebook, the following apply:

The Customer must take such measures as the Corporation or the owner may require to assist it in any actions to register, perfect, maintain, or protect the owners' rights to the Marks. The Customer may be required by the Corporation or the owner to litigate in the Customer'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 the Corporation or the owner. The owner will pay the Customer's out-of-pocket expenses related to these activities.

4.5 Display on Cards

In addition to the Rules in Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook, the following apply:

All Cards must bear the appropriate Marks, which must be on the front of the Card.

The Marks may co-reside on a MasterCard card in the context of a Corporation-approved multi-account card program.

The Marks may co-reside on Cards with other payment scheme marks upon written agreement with the Corporation. If Cards bear multiple payment scheme marks in addition to the Marks, only one of the additional payment scheme marks may be placed on the card front.

Customers may issue Cards only in the same form as the specimen Card approved in writing by the Corporation.

Customers must not use the trademark or tradename of a competing international payment scheme on Cards, unless they have received written permission from the Corporation to do so.

In the EEA, the Marks may be placed on any type of card, including Credit Cards and Commercial Cards.

NOTE

Additional Rules on this topic appear in Section 17b, "Single European Payment Area Rules," of this rulebook.

4.6 Display of the Marks at POI Terminals

In addition to the Rules in Chapter 4, "Marks," Rule 4.6 in part 1 of this rulebook, the following apply:

The minimum size permitted for reproduction of the Marks on or near a POI Terminal is fifty (50) mm in width. The width of the Marks should be measured from left edge to right edge of the blue background box.

The Marks must have equal prominence with international, regional, and bilateral marks displayed on the same POI Terminal.

The Marks must be shown in full-color according to the color specifications, provided by the Corporation.

Display at POS Terminals

Upon request, Acquirers must make artwork or transparencies of advertising material that feature the Marks available to Merchants. Such material is available from the Corporation.

Display at Terminals

The 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 Marks in Advertising

All advertising that makes reference to the Marks must be submitted to the Corporation 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 the Corporation's permission to use the Marks provided that:

1. the Marks do not occupy a prominent position (i.e. not more than ten percent (10%) of advertising space);
2. the Corporation does not appear to endorse a product or service (see "Use of the 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 Marks.

5.1 Special Issuer Programs—General Requirements

In addition to the Rules in Chapter 5, "Special Issuer Programs," Rule 5.1 in part 1 of this rulebook, the following apply:

In the Europe Region, affinity and co-branded Card Programs ("A/CB Card Programs"), which are a subset of Special Issuer Programs, involve the placement on Cards of a trade name, mark, or both, of any entity or group not eligible for License. Cardholder services (for example, assistance services) that are part of a Customer's standard current account package are not considered to be part of affinity or co-branded Card Programs.

Unless specified otherwise, all Rules, regulations, and policies applicable to all other Card issuing Programs, apply at all times to any A/CB Card Program.

The Card must always provide a means to pay for the goods, services, or both supplied by the A/CB Card Program partner.

5.2 Affinity and Co-Brand (A/CB) Card Programs

5.2.2 Program Approval

In addition to the Rules in Chapter 5, "Special Issuer Programs," Rule 5.2 2 in part 1 of this rulebook, the following applies:

If an A/CB Card also carries the logo of a domestic/local acceptance scheme, the Corporation will approve the program only if the domestic/local scheme in which the Card participates has already given its approval.

The Corporation reserves the right to require any Customer to submit all contracts with an A/CB Card Program partner or any other documentation regarding an A/CB Card Program in order to determine compliance with any of the requirements of the Rules.

5.3 A/CB Communication Standards

5.3.1 Standards for All Communications

In addition to the Rules in Chapter 5, "Special Issuer Programs," Rule 5.3.1 in part 1 of this rulebook, the following applies:

If the partner's mark, logo or program name appears as part of any written communication regarding any aspect of the A/CB Card Program, the Issuer's mark/logo or the electronic debit brands must be at least as prominently displayed or mentioned.

5.4 A/CB Card Requirements

5.4.3 A/CB Card Design—Partner's Identification

When placed on the Card front, the name of the A/CB Card program partner(s) may be personalized by means of laser engraving (recommended) or indent printing in the Issuer identification area or the card personalization area. In the card personalization area, the Issuer may optionally use the embossing, thermal transfer or ultragraphics techniques, although these are not advised. The name may be placed in the Card personalization area in addition to, or in lieu of, its use in the upper portion of the Card face. This personalization must be in line with the minimum Card requirements for the personalization area.

5.4.4 A/CB Card Design—Program Names

A program name is a name that distinguishes a Customer's A/CB Card Program from any of the Customer's other Programs and from the Programs of other Customers. Issuers must obtain the Corporation's approval of the A/CB Card program name to be used.

5.7 Chip-only Card Programs

An Issuer may issue "Chip-only Cards", defined herein as Chip Cards for which the presence of a magnetic stripe is optional, or if the Card has a magnetic stripe, the presence of the Maestro payment application on the magnetic stripe is optional, subject to the following conditions:

1. The Corporation must approve, in writing and in advance of Program launch, any Chip-only Card Program and each Card design to be used in connection with a Chip-only Card Program.
2. The Corporation must approve separately each Card design to be used in connection with a Chip-only Card Program.
3. The Account range used for a Chip-only Card Program must be separate from any Account range used for the issuance of other Cards, unless otherwise agreed with the Corporation.
4. The PAN on Chip-only Cards must not be embossed, as set forth in Rule 6.2.2 of this Chapter 19.
5. In a Card-present environment, the Issuer must authorize solely Chip Transactions on a Chip-only Card. If the Card has a magnetic stripe containing the Maestro payment application, the Issuer must decline all magnetic stripe Transactions on the Card.
6. The geographic scope of acceptance of a Chip-only Card Program must be limited to the Europe Region. The geographic restriction must be clearly printed on the Card front, for example "Valid only in Europe".

7. The Issuer must inform the Cardholder clearly in writing of the limitations on acceptance of the Card.
8. The Issuer must communicate the option of receiving an unrestricted Card to all Chip-only Card Program Cardholders and provide such a Card to any Cardholder who requests one.
9. The Issuer must submit and obtain the Corporation's written approval prior to final production and use of all Cardholder communication materials.

6.1 Eligibility

6.1.1 Eligible Cards

The following Rule replaces Chapter 6, "Issuing," Rule 6.1.1, in part 1 of this rulebook:

A Customer may place the Marks on a MasterCard card that gives access to a credit account in the context of a Corporation-approved multi-account Card Program.

In the EEA, the following Rule replaces Chapter 6, "Issuing," Rule 6.1.1, in part 1 of this rulebook:

1. The Issuer is not required to maintain the Account, but must maintain the information necessary to process Transactions initiated by the Cardholder.
2. Issuers may place the Marks on any type of Card, including Cards issued under Special Issuer Programs that have received written approval from the Corporation. (See Chapter 5, "Special Issuer Programs," of this rulebook and applicable regional Rules for further information about affinity co-branded Cards.)

All Cards must conform to the MasterCard Card Design Standards available on MasterCard Connect.

6.1.3 Eligible Accounts

The following Rule replaces Chapter 6, "Issuing," Rule 6.1.3, in part 1 of this rulebook:

Except in the EEA, Cards bearing the Marks must be linked to a sight deposit account or to a pooled account (linked to a Corporation-approved prepaid card program).

Cards bearing the Marks may also be linked to a MasterCard credit account in the context of a Corporation approved multi-account card program, it being understood that the account accessed via the Marks must nevertheless fulfill the requirement in the preceding paragraph.

In the EEA, Cards bearing the Marks must be linked to an Account.

6.1.4 Program Names

An Issuer may apply to the Corporation for permission to have a Card Program name appear in addition to or in lieu of the Issuer name or any Affinity or Co-brand Card Program partner's name or both on the Card face and, with such permission, may use such a Card Program name. Each Card Program name, offering, and service must be referred to by the full, legal name and include the appropriate registration notice.

6.2 Card Standards and Specifications

In addition to the Rule in Chapter 6, "Issuing," Rule 6.2 in part 1 of this rulebook, the following applies:

Customers may apply to the Corporation for BIN/IINs, or they may use current BIN/IINs.

The 639000 to 639099 and 670000 to 679999 BIN ranges are reserved for the sole use of the Corporation. BINs from these ranges are assigned to Customers for the issuance of Cards and may not be used for any other purpose without the written agreement of the Corporation. The 639000 to 639099 and 670000 to 679999 BIN ranges must not be used to issue cards bearing competing global or regional brands. Refer to Rule 4.5 regarding the display of the Marks and other marks on Cards.

6.2.1 Encoding Standards

6.2.1.9 Encoding of PIN Verification Value (PVV)

In addition to the Rules in Chapter 6, "Issuing," Rule 6.2.1.9 in part 1 of this rulebook, the following apply:

Cards with a bank-owned PVV or without PVV can only be authorized by the Issuer.

If PVV is encoded, the Issuer can use the PVV verification offered by the Dual Message System (that is, PIN validation in Stand-In and PIN pre-validation services). Please refer to the *On Behalf Key Management (OBKM) Document Set* for more detailed information about exchanging PIN validation keys.

6.2.1.10 Track 3

If a Card has track 3 encoded, the encoding must conform to ISO 4909 "Bank cards–Magnetic stripe content for track 3."

6.2.2 Embossing and Engraving Standards

The following replaces Chapter 6, "Issuing," Rule 6.2.2 (3) in part 1 of this rulebook:

1. It is strongly recommended that an Issuer customer service phone number be printed on the Card back.
2. The PAN on Chip-only Cards, as described in Rule 5.7 of this Chapter 17, must not be embossed.

NOTE

A Rule variation on this topic appears in Section 17b, "Single European Payment Area Rules," of this rulebook.

6.2.3 Chip Card Standards

Any Chip Card, except for Chip Cards that support online-only authorization, issued on or after 1 January 2011:

1. Must support offline DDA CAM;
2. Must not support offline SDA CAM.
3. Chip Cards may support offline CDA CAM.

NOTE

Additional Rules on this topic appear in Section 17b, "Single European Payment Area Rules," of this rulebook.

6.2.3.4 Chip Card and Chip Transaction Plans

Customers must provide to the Corporation the following information on their plans to issue Chip Cards or acquire chip Transactions or both:

1. Number of Chip Cards; and
2. Number of hybrid POS Terminals and Terminals.

6.3 Optional Card Security Features

NOTE

Additional Rules on this topic appear in Section 17a, "UK Maestro Intracountry Rules," of this rulebook

6.4 PIN and Signature Requirements

In addition to the Rules in Chapter 6, "Issuing," Rule 6.4 in part 1 of this rulebook, the following applies:

Cardholders must be verified by a PIN for Maestro *PayPass* Transactions that exceed the applicable Transaction amount ceiling limit.

6.4.2 Use of the PIN

6.4.2.1 Chip Cards

In addition to the Rules in Chapter 6, "Issuing," Rule 6.4.2.1 in part 1 of this rulebook, the following applies:

4. Chip Cards must support online PIN verification as the CVM for Maestro *PayPass* Transactions initiated with a Card that exceed the applicable Transaction amount ceiling limit.

6.4.3 Use of PIN or Signature

NOTE

Additional Rules on this topic appear in Section 17b, "Single European Payment Area Rules," of this rulebook

6.4.4 Liability Shift for Signature-based Transactions at Magnetic Stripe Reading-Only POS Terminals

Issuers may charge back under reason code 4837 all fraudulent intraregional Transactions completed using signature as the CVM at magnetic stripe reading-only POS Terminals.

Refer to Appendix B of the *Chargeback Guide* for further information.

6.4.5 For ATM and PIN-based In-Branch Terminal Transactions

Cardholders undertaking magnetic stripe Transactions must be verified by means of online PIN verification.

Chip

In the case of chip Transactions, the Cardholder must be verified by means of online PIN verification.

PIN Entry Errors—For All Transactions

Transaction attempts where the PIN is entered incorrectly must be declined. For chip Transactions, the application or the Card may also be blocked if the Cardholder exceeds the number of PIN attempts permitted by the Issuer.

6.9 Electronic Commerce

The following replaces Chapter 6, "Issuing," paragraph two of Rule 6.9 in part 1 of this rulebook:

Issuers in Ireland must allow their cardholders to perform electronic commerce Intracountry Transactions if they allow cardholders to perform electronic commerce transaction under other debit brands.

All Issuers must allow their Cardholders to perform electronic commerce Transactions on all Cards except prepaid Cards. For prepaid Cards, it is strongly recommended that Issuers allow their Cardholders to perform electronic commerce Transactions.

6.9.2 MasterCard Advance Registration Program (MARP) Transactions

Issuers must technically support MasterCard Advance Registration Program (MARP) Transactions on Cards which may be used to perform electronic commerce Transactions. They must make individual authorization decisions and must not automatically decline authorization of MARP transactions on Cards which may be used to perform electronic commerce Transactions.

These Transactions contain a value of 3, 4 or 5 in Data Element 48 (Additional Data—Private Use), subelement 43 (Static AAV for Maestro or MasterCard Advance Registration Program), position 1 of Authorization Request/0100 messages. Refer to the *Customer Interface Specification* manual for further information.

6.10 Selective Authorization

In addition to the Rules in Chapter 6, "Issuing," Rule 6.10 in part 1 of this rulebook, the following applies:

Issuers may geographically restrict Card usage for a particular Card portfolio as a fraud prevention measure, subject to the following requirements:

1. The geographic area in which the Card may be used must be clearly identifiable, for example domestic-only or Europe-only. For Cards issued in SEPA countries, a domestic-only restriction is not permitted.
2. The Issuer must use an Account range for the issuance of geographically restricted Cards that is separate from any Account range used for the issuance of unrestricted Cards, unless otherwise agreed with the Corporation.
3. The geographic restriction must be clearly printed on the Card front, for example "Valid only in Europe."
4. The Card design of geographically restricted Cards must be approved separately by the Corporation.
5. The Issuer must inform the Cardholder clearly in writing of the geographic scope of the Card and of any change in scope.
6. The Issuer must communicate that the Cardholder has the option of receiving a Card with no geographic restriction to all of its Cardholders and provide such a Card to any Cardholder who requests one.
7. The Issuer must obtain the Corporation's prior written approval of all Cardholder communication materials.

6.11 MasterCard *MoneySend* Payment Transaction

In addition to the rules in Chapter 6, "Issuing", Rule 6.11 in part 1 of this rulebook, the following apply.

All Issuers in the countries listed below must properly process and authorize MasterCard® *MoneySend*™ Payment Transactions.

6.11.1 MasterCard *MoneySend* Payment Transaction Requirements

In the countries listed below, paragraph 1 of Rule 6.11.1 in Chapter 6 in part 1 of this rulebook does not apply in that Issuers are not required to register.

Albania	Georgia	Poland
Armenia	Hungary	Romania
Azerbaijan	Israel	Russian Federation
Belarus	Kazakhstan	Serbia
Bosnia and Herzegovina	Kosovo	Slovakia
Bulgaria	Macedonia	Slovenia

Croatia	Malta	Turkey
Cyprus	Moldova	Ukraine
Czech Republic	Montenegro	

In the countries listed above, the following replaces paragraph 5 of Rule 6.11.1 in part 1 of this rulebook:

The Issuer receiving a MasterCard *MoneySend* Payment Transaction authorization request:

1. may approve or reject any requests by the Acquirer to correct a clerical error; and
2. must not establish its own maximum MasterCard *MoneySend* Payment Transaction amount.

The Issuer must make the transferred funds available to the Cardholder promptly upon approval of the financial authorization request and in the amount indicated in DE 4 (Amount, Transaction) when the Transaction currency matches the currency of the Cardholder's Account.

A MasterCard *MoneySend* Payment Transaction (MCC 6536 or 6537) must be effected in a way that does not conflict with Cardholder agreements or instructions.

6.13 Issuer Responsibilities to Cardholders

In addition to the Rules in Chapter 6, "Issuing," Rule 6.11 of this rulebook, the following apply:

Issuers must provide information to their Cardholders as set forth below, in addition to any information required under applicable law. The Corporation may ask an Issuer to certify its compliance with these Rules.

1. Before the Card is used, Issuers must make information available to their Cardholders as to where the Card may be used (that is, wherever, at home or abroad, the relevant Marks are displayed). Issuers must also provide the following information to their Cardholders:

   a. the price of the Card;

   b. specific charges, if any, to be paid to the Issuer for the kind(s) of service (both at home and abroad) provided through the Card. Examples of these charges are; cash advance fee, ATM usage fee, and interest rates to be applied;

   c. the basis for calculation of the exchange rate;

   d. notice that exchange rates can fluctuate and that they may change between the time when the Transaction is made and the time when it is billed to the Cardholder's Account;

   e. the Cardholder's liability, including the cost, if the Card is lost or stolen. This information must be stated clearly in the body of the product literature. The Cardholder must also be told what to do if the Card is lost or stolen;

   f. the standard limit, if any, up to which the Cardholder can use the Card;

   g. when the Transaction is likely to be billed to the Cardholder's Account; and

   h. information required to be provided by Rule 3.22.3 of this chapter.

2. At the time of billing the Transaction, as applicable, the following information must be provided to the Cardholder:

   a. Transaction type (for example, ATM cash withdrawal, cash advance) and location (if technically feasible);

   b. amount in Transaction currency;

   c. amount in billing currency;

   d. exchange rate applied;

   e. total commission applied (if applicable);

   f. interest rate applied (if applicable).

6.13.1 Limitation of Liability of Cardholders for Unauthorized Use

This Rule applies with respect to Cards issued in EEA countries. Cards issued to an entity other than a natural person are excluded, unless otherwise provided by applicable law or the Cardholder agreement.

With respect to Cards issued in countries other than EEA countries, this Rule is a recommendation rather than a mandate.

For Transactions that have not been authorized by the Cardholder (for example, fraudulent Transactions), the Cardholder's liability is **zero**, except as set forth below.

Lost and Stolen Fraud. In the case of fraudulent Transactions resulting from loss or theft of the Card, the Cardholder's liability is limited to a maximum of **EUR 150**, or to a lesser amount if so specified in applicable law or in the Cardholder agreement, for unauthorized use of the Card occurring **before** notification by the Cardholder of the loss or theft. If the Cardholder has acted fraudulently or with intentional or gross negligence, or has delayed unduly in notifying the Issuer or the entity specified by the Issuer of the loss or theft, the Cardholder's liability for fraudulent Transactions resulting from loss or theft of the Card, and occurring prior to notification, is not limited.

The Cardholder's liability for fraudulent Transactions resulting from loss or theft of the Card is **zero** as from the time when the Cardholder has notified the Issuer or the entity specified by the Issuer of the loss or theft, or if the Issuer fails to provide means for the notification at all times of loss or theft. If the Cardholder has acted fraudulently, zero liability does not apply.

Upon the Cardholder's request, the Issuer must provide proof to the Cardholder of the notification of loss or theft of the Card during a period of 18 months after notification.

6.14 Fraud Reporting

6.14.1 Reporting

In addition to the Rules in Chapter 6, "Issuing," Rule 6.14.1 in part 1 of this rulebook, the following apply:

The obligation to report fraudulent Transactions applies to Principals, with respect to themselves and their Affiliates.

All fraudulent Transactions (international, domestic and on-us) must be reported.

6.16 Co-residing Applications

The following additional Rules apply in the Europe Region.

Co-residing applications are Customer or third party proprietary applications or functions, unrelated to the Corporation, which co-reside on Cards.

Customers' proprietary domestic payment functions or brands, whether stored-value, debit or credit, are co-residing applications if they reside on a chip itself embedded on Cards. If these functions do not reside on the chip, the Rules on co-residing applications do not apply.

6.16.1 General Requirements

Customers may not use the Marks as part of the identification of any co-residing application without the Corporation's prior written approval.

Co-residing payment applications may not use or be associated with any competitive brand (*e.g.* American Express, JCB, Diners Club, and Visa).

Co-residing applications must not damage the Marks. Co-residing applications must not have a negative impact on the interoperability of the MasterCard brands.

Customers must implement all measures necessary to avoid interference by co-residing applications with any applications represented by the Marks.

6.16.2 Notification

The Corporation must be notified of co-residing payment applications by submission of the notification form in Appendix D, "Forms." Co-residing applications used solely for non-payment purposes, such as identification or access, do not have to be notified.

A Principal may notify co-residing applications on behalf of its Sponsored Affiliates.

If a co-residing payment application is discontinued, the Issuer must notify the Corporation without delay.

6.17 Additional Rules for Issuing

The following additional Rules apply in the Europe Region.

An Issuer is responsible for the issuing of Cards and PINs to its Cardholders and performing Cardholder Account maintenance. Additionally, an Issuer must:

1. perform secure Card management, including Card re-issue and PIN allocation and distribution;
2. take all reasonable steps to ensure that all its Cardholders are able to use their Cards at all POI Terminals;
3. provide authorization systems to process and respond to authorization requests relating to Transactions on the Issuer's Cards. Support of a "dynamic stand-in" facility is available; and
4. ensure that all Cards issued bear a signature stripe or have a laser-engraved signature, and must issue a PIN unless the Cardholder requests otherwise.

6.19 Recurring Payments

Issuers must allow their Cardholders to perform recurring payment Transactions as either face-to-face or electronic commerce recurring payment Transactions on all Cards except prepaid Cards and must recognize properly identified recurring payment Transactions.

For prepaid Cards, it is strongly recommended that Issuers allow their Cardholders to perform recurring payment Transactions.

The following applies to intracountry recurring payment Transactions occurring within France, Hungary, Ireland, Poland, Romania, Ukraine, and the United Kingdom:

An Issuer must not decline a non-face-to-face recurring payment Transaction from a Merchant solely on the basis of missing Card expiration date information.

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," Rule 7.1.1.2 in part 1 of this rulebook, the following apply:

1. 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
2. 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.
3. Acquirers must terminate Merchant agreements promptly with Merchants who do not conform to the Standards. This conformity must include:
   a. application of the security and authorization procedures;
   b. compliance of POS Terminals to the Corporation's POS Terminal specifications.
4. In the EEA, each Merchant agreement must contain a term requiring the Merchant to respond to Cardholder disputes and handle chargebacks in accordance with the *Chargeback Guide*.

Acquirers may be instructed to terminate merchant agreements.

7.1.3 Use of a Payment Facilitator

7.1.3.1 Responsibility for Payment Facilitator and Sub-merchant Activity

If a Payment Facilitator or Sub-merchant is located in a country for which the Acquirer has central acquiring authorization in accordance with Rule 2.3.3 of this Chapter 17, the Acquirer is not required to also obtain a License or an Extension of Area of Use covering the same country. If a Payment Facilitator or Sub-merchant is located in a country that is not one of the Western or Central European countries listed in Rule 2.3.3.4, the central acquiring authorization must specifically mention the Payment Facilitator and/or Sub-merchant.

7.1.5 Acquiring Transactions

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.1.5 in part 1 of this rulebook, Acquirers must:

1. supply the Merchant with Merchant Operating Guidelines relevant to the type of Merchant and the type of POS Terminal(s) installed;
2. allocate each outlet with a merchant category code (MCC) and an outlet identity.

7.1.7 Transmitting and Processing Transactions

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.1.7 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.

7.1.15 Information to Merchants—European Economic Area Only

An Acquirer:

1. must inform existing and prospective Merchants that interchange fees and Rules set by the Corporation are available on the MasterCard public Internet site (www.mastercard.com);
2. must inform existing and prospective Merchants that they may apply different surcharges to Transactions, MasterCard credit card transactions, MasterCard commercial card transactions and MasterCard debit card transactions, while respecting Rule 7.2.2 (Merchant Surcharging) of this chapter.
3. must inform existing and prospective Merchants that they are not obliged to accept MasterCard cards and/or the cards of any other network as a condition for accepting Cards;
4. may not prohibit existing or prospective Merchants from entering into a merchant agreement with any other Acquirer with respect to Transactions, MasterCard credit card transactions, MasterCard commercial card transactions, MasterCard debit card transactions and/or the transactions of other card networks, unless the Merchant elects to enter into a Merchant agreement solely with the Acquirer;
5. must provide to existing and prospective Merchants pricing information that specifies separately (including separately from that of any other card network) the financial terms to be applied to Transactions, MasterCard credit card transactions, MasterCard commercial card transactions and MasterCard debit card transactions, unless the Merchant elects that the Acquirer shall not have to provide such separate pricing information; and
6. must indicate on Merchant invoices the number of Transactions, Volume and total amount of the Merchant service charge separately (including separately from those of any other card network) for Transactions, MasterCard credit card transactions, MasterCard commercial card transactions and MasterCard debit card transactions, unless the Merchant elects that the Acquirer shall not have to provide such separate invoice information.

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," Rule 7.2 in part 1 of this rulebook, the following applies:

16. ensure that Merchants submit recurring payment Transactions only after they have been registered and received a Corporation-assigned Merchant ID and static AAV.

17. provide Cardholders the option to register for recurring payment Transactions when such Transactions are offered by the Merchant.

The following applies to intracountry recurring payment Transactions occurring within France, Hungary, Ireland, Poland, Romania, Ukraine, and the United Kingdom:

The Acquirer is recommended to ensure that the Merchant only includes the Card expiration date in the first Transaction of a recurring payment arrangement involving a particular Card account number. The Corporation recommends that the Card's expiration date is not included in any subsequent recurring payment Transaction authorization requests involving the same PAN.

7.2.1 Merchant Surcharging

The following Rule replaces Chapter 7, "Acquiring," Rule 7.2.1 in part 1 of this rulebook:

The prohibition on Merchant surcharging in Rule 7.2.1 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.

7.3 Additional Acquirer Obligations and Activities for Terminals

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.3 in part 1 of this rulebook, the following applies:

Acquirers may optionally choose to provide the PIN-based cash withdrawal service in their branches; the extent of the service to be determined in their business plan.

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 Rule 2.3.3 of this chapter.

7.5 Acquiring Payment Transactions

Refer to Rule 9.4.8 in this chapter for rules on the Gaming Payment Transaction.

In addition to part (e) of the Rules in Chapter 7, "Acquiring," Rule 7.5 in part 1 of this rulebook, the following applies:

With respect to an interregional Payment Transaction involving a Europe region Acquirer and an Issuer located in another region, if the Acquirer does not submit a clearing message to the Interchange System within seven (7) days of the authorization request, the Corporation will collect the Payment Transaction amount and any additional fees charged from the Acquirer by means of a Fee Collection/1740 message.

7.6 Acquiring MasterCard *MoneySend* Payment Transactions

The following rule variations apply for domestic MasterCard *MoneySend* Payment Transactions in Russia.

Cash and any type of anonymous prepaid card, e-wallet or other anonymous funding source may be used as the source of funding for a MasterCard *MoneySend* Payment Transaction, provided that the Transaction amount does not exceed RUB 15,000. The Transaction may be completed face-to-face, at any unattended POI Terminal capable of processing the Transaction or non–face-to-face. It is not required to verify the sender's identity.

Originating institutions must report on the number and financial value of anonymously funded and cash-funded MasterCard *MoneySend* Payment Transactions. The report must be sent on a quarterly basis to the local MasterCard representative for the originating institution.

7.9 POS Terminal and Terminal Requirements

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.9 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.

7.9.2 Manual Key-entry of PAN

The following is an exception to the Rule in Chapter 7, "Acquiring," Rule 7.9.2 in part 1 of this rulebook:

MO/TO refund Transactions may be processed to Cards using manual key entry of the PAN.

7.9.4 Function Keys

The following replaces the Rule in Chapter 7, "Acquiring," Rule 7.9.4 paragraph 1 in part 1 of this rulebook:

The function key to terminate a Transaction is mandatory.

7.9.7 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:

1. 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;
2. 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.

7.10 Hybrid POS Terminal and Hybrid Terminal Requirements

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.10 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.

NOTE

Additional Rules on this topic appear in Section 17b, "Single European Payment Area Rules," of this rulebook.

7.10.1 Chip Liability Shift

The liability for Europe intraregional counterfeit Transactions in which one Customer (either the Issuer or the Acquirer) is not yet EMV-compliant will be borne by the non-EMV-compliant party in the Transaction process.

The chip liability shift is implemented in reason code 4870. Refer to Appendix B of the *Chargeback Guide* for further information.

Magnetic Stripe Reading-Only POS Terminals

If the original hybrid Card was issued with an EMV-compliant chip and if the magnetic stripe reading-only POS Terminal supports online PIN, the chip liability shift applies only to counterfeit fraudulent Transactions.

If the original hybrid Card was issued with an EMV-compliant chip and if the magnetic stripe reading only POS Terminal is in a Waiver country (Chapter 6, "Issuing," Rule 6.4.3 in part 1 of this rulebook) and does not support online PIN verification, the chip liability shift applies to all types of fraudulent Transactions completed with signature as the CVM.

7.11 Additional Requirements for POS Terminals

7.11.1 Additional Requirements for Hybrid POS Terminals

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.11.1 in part 1 of this rulebook, the following applies:

3. POS Terminals that are online PIN-capable must support online PIN as the CVM for Maestro *PayPass* Transactions that exceed the applicable Transaction amount ceiling limit. Maestro *PayPass* Transactions that exceed the ceiling limit must not be completed at POS Terminals that are not online PIN-capable; a contact Transaction may instead be completed when the Transaction amount exceeds the *PayPass* ceiling limit. It is strongly recommended that such POS Terminals also support offline verification of the mobile PIN for Maestro *PayPass* Transactions initiated with a Mobile Payment Device that exceed the applicable Transaction amount ceiling limit.

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, Rule 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 Waiver country (refer to Part 1, Rule 6.4.3).

POS Terminals located in the Europe region should support technical fallback during the initial stages of a merchant's chip migration.

Acquirers may withdraw support for technical fallback at POS Terminals deployed within a market as the market matures and the Acquirer is content that technical fallback support is no longer required to ensure good customer service. Upon withdrawing fallback support at a POS Terminal, the Acquirer must ensure that the POS Terminal continues to support magnetic stripe Card acceptance.

The Issuer does not have the right to charge back under reason codes 4837 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.

7.11.2 Hybrid POS Terminal CAM Policy

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.11.2 in part 1 of this rulebook, the following applies:

All online capable hybrid POS Terminals must support dynamic online CAM.

7.12 Additional Requirements for ATMs

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.12 in part 1 of this rulebook, the following apply:

Screens

Both single-line and multi-line screens are acceptable. A minimum screen width of forty (40) characters is recommended. Refer to Appendix D of this rulebook, for recommended screen messages.

Minimum Withdrawal Amount

Each ATM must be capable of dispensing, without limit per Transaction, the authorized amount requested by the Cardholder, unless for technical and/or security reasons the amount per Transaction is limited to at least EUR 200 or the equivalent in local currency.

Currency

An Acquirer may dispense in its ATMs currency other than the local currency, provided that the following conditions are met:

1. the Cardholder is informed of the currency that the ATM will dispense before the Transaction is made; and
2. if a receipt is provided, it will mention the currency concerned.

7.12.1 Additional Requirements for Hybrid ATMs

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.12.1 in part 1 of this rulebook, the following apply:

Chip

ATMs may support chip technology. Any ATM that supports chip technology must also support magnetic stripe technology.

If the ATM supports chip technology, the chip must be read and processed in accordance with the chip technical specifications.

All ATM Transactions must be authorized online to Issuer, whether the magnetic stripe or the chip is used to initiate the Transaction. ATM Transactions may not be authorized offline by the chip in the event that an online authorization cannot be completed for technical reasons.

Technical Fallback

If both the Card and the ATM support chip technology, the Transaction may only be completed using the chip. Fallback to magnetic stripe is not permitted.

7.12.1.1 Hybrid ATM CAM Policy

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.12.1.1 in part 1 of this rulebook, the following applies:

All hybrid ATMs must support dynamic online CAM.

7.13 Additional Requirements for PIN-based In-Branch Terminals

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.13 in part 1 of this rulebook, the following apply:

Screens
Both single-line and multi-line screens are acceptable. A minimum screen width of forty (40) characters is recommended. Refer to Appendix D, "Signage, Screen, and Receipt Test Displays," for recommended screen messages.

Minimum Withdrawal Amount

Each PIN-based In-Branch Terminal must be capable of dispensing, without limit per Transaction, the authorized amount requested by the Cardholder unless for technical and/or security considerations/constraints, the amount per Transaction is limited to at least the equivalent of EUR 200 in local currency.

7.13.1 Additional Requirements for Hybrid PIN-based In-Branch Terminals

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.13.1 in part 1 of this rulebook, the following apply:

Chip

All PIN-based In-Branch Terminals must comply with the requirements set forth in Rule 7.13.1 of this Chapter 17.

Technical Fallback

Technical fallback is permitted at PIN-Based In-Branch Terminals. When technical fallback occurs, PIN must be used as the CVM.

Acquirers may withdraw support for technical fallback at PIN-Based In-Branch Terminals deployed within a market as the market matures and the Acquirer is content that technical fallback support is no longer required to ensure good customer service. Upon withdrawing fallback support at a PIN-Based In-Branch Terminal, the Acquirer must ensure that the PIN-Based In-Branch Terminal continues to support magnetic stripe Card acceptance.

7.13.1.1 Hybrid PIN-based In-Branch Terminal CAM Policy

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.13.1.1 in part 1 of this rulebook, the following applies:

All hybrid PIN-based In-Branch Terminals must support dynamic online CAM.

7.14 POI Terminal Transaction Log

The exception for Merchant-approved transactions set forth in part 1 of this rulebook does not apply for Merchant-approved Transactions acquired in the Europe Region. Such Transactions may not be resubmitted after the Issuer has declined them.

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.14 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 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.

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.

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)
- PAN, card sequence number, and expiration date
- Transaction number
- Authorization response identifier.

For chip Transactions, Acquirer Transaction records should additionally contain the Transaction's cryptogram and related data elements.

7.15 Requirements for Transaction Receipts

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.15 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.

7.15.1 Receipt Contents for POS Terminals

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.15.1 in part 1 of this rulebook, the following apply:

The Transaction receipt should contain the following data:

Merchant Details

1. Merchant identification (mandatory)
2. Merchant trading address (optional)
3. Merchant outlet identifier (Acquirer's) (mandatory)
4. VAT registration number (optional)

Card Scheme Details

1. space for card scheme name—'Maestro' (configurable) (mandatory)

Transaction Details

1. local date and time of the Acquirer (DD/MM/YY, HH.MM - 24 hr) (mandatory)
2. Transaction printout (receipt) number (optional)
3. POS Terminal identification (mandatory)
4. POS Terminal location (name, city, country) (mandatory)
5. Transaction type (*e.g.* purchase, refund) (mandatory)
6. amount (mandatory)
7. unique Transaction number (mandatory)
8. authorization response identification (mandatory)
9. currency denomination (mandatory)
10. 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

1. PAN recommended (must be truncated if included)
2. expiration date (recommended)
3. card sequence number (optional). Other discretionary data is not allowed.

Cardholder Interface Details (optional, variable)

1. Message to Cardholder:
   a. "Your account will be debited/credited with the above amount";
   b. "Transaction confirmed";
   c. "……." Cardholder signature (mandatory for signature-based POS Terminals);
   d. "Please keep this copy."
2. Thank you message

7.15.6 PAN Truncation Requirements

7.15.6.1 POS Terminals

In the Netherlands, the following replaces Chapter 7, "Acquiring," Rule 7.15.6.1, in part 1 of this rulebook:

The Cardholder and Merchant receipts generated by all POS Terminals, whether attended or unattended, must omit the Card expiration date. In addition, the Cardholder receipt generated by all POS Terminals, whether attended or unattended, must reflect only the last four (4) digits of the PAN or digits thirteen (13) through sixteen (16) of a nineteen (19)-digit PAN. All other digits of the PAN must be replaced with fill characters that are neither blank spaces nor numeric characters, such as "x," "*,"or "#".

The Corporation strongly recommends that if a POS Terminal generates a Merchant copy of the Cardholder receipt, the Merchant copy should also reflect only the last four (4) digits of the PAN or digits thirteen (13) through sixteen (16) of a nineteen (19)-digit PAN, replacing all other digits with fill characters that are neither blank spaces nor numeric characters, such as "X," "*," or "#."

7.17 Connection to the Interchange System

NOTE

A Rule variation on this topic appears in Section 17b, "Single European Payment Area Rules," of this rulebook.

7.17.3 Certification

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.17.3 in part 1 of this rulebook, the following applies:

Prior to issuing Chip Cards or accepting chip Transactions, Customers must successfully pass an end-to-end acceptance test, which will be conducted by the Corporation, in a live environment, even if they previously participated in the Interchange System.

7.18 Card Capture

7.18.2 ATM Transactions

The following Rule replaces Chapter 7, "Acquiring," Rule 7.18.2 paragraph 1 in part 1 of this rulebook:

Terminal owners are required to honor Card capture commands at all Terminals that are capable of Card capture from all Issuers.

7.18.2.3 Disposition of Suspicious Captured Cards

The following Rules replace Chapter 7, "Acquiring," Rule 7.18.2.3 in part 1 of this rulebook:

A magnetic stripe of a non-European Card must be destroyed by cutting in half through the magnetic stripe and the Card should be disposed of. However, if it is obvious that the captured Card is fraudulent (i.e. white plastic), the Acquirer must return the Card without cutting it in half to MasterCard Europe, Fraud and Security Department.

7.20 Merchandise Transactions

7.20.1 Approved Merchandise Categories

In addition to the Approved Merchandise Categories listed in Chapter 7, "Acquiring," Rule 7.20.1 of this rulebook, the following applies:

Merchandise Category	Explanation
Mobile Phone Top Up	A specified amount of prepaid wireless telephone time, to be credited to the mobile SIM card associated with the subscriber's prepaid telephone account.
Bill Payment	Payment via the ATM of utility, telephone or other bills. The Transaction may be identified with MCC 4900 or MCC 6050.

7.23 ATM Access Fees

7.23.1 Domestic Transactions

The following Rules replace Chapter 7, "Acquiring," Rule 7.23.1, paragraph 1 in part 1 of this rulebook:

Upon complying with the ATM Access Fee notification requirements of the Rules, Acquirers in the United Kingdom may assess an ATM Access Fee on a Transaction initiated with a Card that was issued in the United Kingdom so long as the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory fashion.

Acquirers in the United Kingdom must not assess an ATM Access Fee on non-financial (anything other than a cash withdrawal) Transactions.

7.23.1.1 Transaction Field Specifications

At the time of each cash withdrawal Transaction on which an ATM Access Fee is imposed, the Acquirer of such Transaction must transmit, in the field specified in the applicable technical specifications manual(s) then in effect, the amount of the ATM Access Fee separately from the amount of the cash disbursed in connection with such Transaction.

7.23.1.2 Notification of ATM Access Fee

An Acquirer that plans to add an ATM Access Fee must notify its Sponsoring Principal, in writing, of its intent to do so prior to the planned first imposition of such ATM Access Fee by the Acquirer.

The Principal must update the Location Administration Tool (LAT) regarding its or its Affiliates' imposition of ATM Access Fees.

7.23.1.3 Cancellation of Transaction

Any Acquirer that plans to add an ATM Access Fee must notify the Cardholder with a screen display that states the ATM Access Fee policy and provides the Cardholder with an option to cancel the requested Transaction.

7.23.1.4 Terminal Signage, Screen Display, and Receipt Requirements

An Acquirer that plans to add an ATM Access Fee to a Transaction must submit proposed Terminal signage, screen display, and receipt copy that meets the requirements of the Rules to its Sponsoring Principal in writing for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook).

The Sponsoring Principal has the right to determine the acceptability of any new or changes to previously approved Terminal signage, screen display, and receipt copy. In cases of conflict between the Acquirer and its Sponsoring Principal, the Corporation has the sole right to determine the acceptability of any and all Terminal signage, screen display, and receipt copy.

7.23.1.4.1 Additional Requirements for Terminal Signage

An Acquirer that plans to add an ATM Access Fee to a Transaction may optionally display signage that is clearly visible to Cardholders on or near all Terminals at which ATM Access Fees apply.

The minimum requirement for ATM Access Fee Terminal signage text is wording that clearly states:

1. the name of the ATM Owner and Principal;
2. that the Transaction may be subject to an ATM Access Fee that will be deducted from the Cardholder's Account in addition to any Issuer fees;
3. the amount of, calculation method of, or Corporation-approved generic signage regarding the ATM Access Fee;
4. that the ATM Access Fee is assessed by the Acquirer instead of the Issuer; and
5. that the ATM Access Fee is assessed on United Kingdom Cardholders only

The minimum requirements for Terminal signage (physical characteristics) are as follows:

1. the signage must bear the heading "Fee Notice";
2. the size of the Terminal signage must be a minimum of ten (10) centimeters in height by ten (10) centimeters in width;
3. the text must be clearly visible to all. It is recommended that the text be a minimum of fourteen (14) point type;
4. the heading must be clearly visible to all. It is recommended that the text be a minimum of eighteen (18) point type.

A model for Terminal signage regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.1.4.2 Additional Requirements for Terminal Screen Display

An Acquirer that plans to add an ATM Access Fee to a Transaction must present a screen display message that is clearly visible to Cardholders on all Terminals at which ATM Access Fees apply. If the Cardholder is given the option of choosing a preferred language in which to conduct the Transaction, the screen display message concerning ATM Access Fees must be presented to the Cardholder in that chosen language.

If an Acquirer displays the Corporation-approved generic ATM Access Fee signage, the Acquirer must include the amount of the ATM Access Fee as part of the Terminal screen display.

A model for the Terminal screen display regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.1.4.3 Additional Requirements for Terminal Receipts

An Acquirer that adds an ATM Access Fee to a Transaction must make available to the Cardholder on its Terminal receipt the ATM Access Fee information required below, in addition to any other information the Acquirer elects or is required to provide.

The minimum requirements for the Terminal receipt are:

1. a statement of the amount disbursed to the Cardholder;
2. a statement of the ATM Access Fee amount with language clearly indicating it is a fee imposed by the Acquirer;
3. a separate statement of the combined amount of the ATM Access Fee and the disbursed amount, with language clearly indicating that this amount will be deducted from the Cardholder's Account.

A model for Terminal receipt text regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.27 Identification of *PayPass* Transactions

If a Card bearing a domestic debit brand in addition to the Marks is used to complete a contactless Transaction, and the domestic debit brand does not support the contactless functionality, the Transaction must be identified in all Transaction messages as a Maestro *PayPass* Transaction and all Rules regarding such Transactions will apply to it.

If the Interchange System is used for processing, the Maestro *PayPass* Transaction is identified by the following data elements:

- Authorization
  - DE 22 (POS entry mode), subfield 1 (POS Terminal PAN Entry Mode) must contain the value of "7" to indicate PAN auto-entry via contactless M/Chip.
  - DE 61 (POS Data), subfield 11 (POS Card Data Terminal Input Capability) must contain the value of "3" to indicate contactless M/Chip
- Clearing
  - DE 22 (POS entry mode), subfield 1 (Terminal Data: Card Data Input Capability) must contain the value of "M" to indicate PAN auto-entry via contactless M/Chip
  - DE 22 (POS data), subfield 7 (Card Data: Input Mode) must contain the value of "M" to indicate PAN auto-entry via contactless M/Chip

If the Transaction is processed via a different network or processing arrangement than the Interchange System (including bilateral and on-us processing), the Acquirer must ensure that corresponding data elements contain values that allow issuers to clearly identify the Transaction as a Maestro *PayPass* Transaction.

Regardless of processing arrangement, all Customers using the *PayPass* technology must have been granted the appropriate *PayPass* licenses as required in Chapter 21 of this rulebook.

8.4 PIN and Key Management Security Requirements

8.4.1 PIN Verification

In addition to the Rules in Chapter 8, "Security," Rule 8.4.1 in part 1 of this rulebook, the following apply:

Refer to the *Authorization Manual*, Chapter 12, "PIN Processing for Europe Region Customers" for information about PIN validation by the Dual Message System in the Europe region.

8.4.2 Stand-In Authorization

If authorization is done by the Dual Message System on behalf of the Issuer, the identification of the Cardholder is based on a cryptographic transformation performed in the MasterCard Host Security Module of data encoded on ISO track 2 in combination with the PIN entered by the Cardholder. The algorithm produces a PIN Verification Value (PVV) that is to be compared with the value obtained from the Card. Positive identification is achieved if both values are identical.

To verify a PIN, the following Card data must be present:

1. PAN; and
2. expiration year and month.

8.9 Account Data Compromise Events

8.9.4 Corporation Determination of ADC Event or Potential ADC Event

8.9.4.2 Potential Reduction of Financial Responsibility

In addition to the Rules in Chapter 8, "Security," Rule 8.9.4.2 in part 1 of this rulebook, the following applies:

8. A PCI SSC Forensic Investigator (PFI) has validated that the Merchant was compliant with milestones one through four of the PCI DSS Prioritized Approach at the time of the ADC Event or Potential ADC Event.

8.13 Signature-based Transactions

8.13.1 Introduction

Cardholder verification is performed using a signature, which must be verified by the Merchant. For refund Transactions, the receipt must be signed by the Merchant rather than the Cardholder.

8.13.2 Certification

The security certification report must indicate which cryptographic techniques are used to obtain security services such as entity authentication, data confidentiality or protection against unauthorized modification, deletion or injection of messages.

The general security requirements for secure cryptographic devices, key management and operational procedures listed in the section entitled "PIN and Key Security Requirements," in Chapter 8 in part 1 and in this Chapter 17 in part 2 of this rulebook apply.

8.13.3 Signature-based POS Terminals

Signature-based POS Terminals must comply with the following requirements:

1. if the signature is unsatisfactory, the Merchant must be able to indicate the cancellation of the Transaction to the POS Terminal, or perform a refund;
2. in case of temporary printer malfunction, the POS Terminal should be able to reprint the receipt, preferably including a duplicate statement, without repeating the Transaction process;
3. the POS Terminal must be designed to protect the Cardholder from deception with regard to:
   a. the fact that no PIN is required;
   b. the normal sequence of Transaction steps;
   c. the information printed or displayed;
   d. additional data requested;
   e. the authorization response;
   f. the completion or cancellation of the Transaction.

8.14 Audit Trail

The following additional Rules apply in the Europe Region.

Systems must be designed and built in such a way that violation of any security requirement can be monitored.

The party responsible for maintaining a particular security function must keep a record of all violations or fraud attempts and the action taken for at least one (1) year.

8.15 Inspection of Customers

The following additional Rules apply in the Europe Region.

Customers must at all times comply with all minimum security Standards with respect to the treatment and safeguarding of card manufacture, printing, embossing, encoding, and mailing as well as for any phase of the production and distribution of Cards or Account information.

Additionally, each Customer must at all times ensure that reasonable means are employed to ensure that Cardholder and Account information is stored and used in a secure manner designed to minimize the likelihood of internal theft or misuse.

Customers must promptly implement such safeguards as the payment scheme may reasonably require to ensure compliance with the aforementioned obligations.

The Corporation has the right to inspect Customers.

9.2 POS Transaction Types

9.2.1 Issuer Online POS Transactions

The Rules set forth in Chapter 9, "Processing Requirements," Rule 9.2.1 in part 1 of this rulebook are modified as shown below:

'Account selection' is not currently supported within the Europe region.

Issuers in the countries listed below are required to offer the MasterCard *MoneySend* Payment Transaction type to their Cardholders.

Albania	Hungary	Romania
Armenia	Israel	Russian Federation
Azerbaijan	Kazakhstan	Serbia

Bosnia and Herzegovina	Kosovo	Slovakia
Bulgaria	Macedonia	Slovenia
Croatia	Malta	Turkey
Cyprus	Moldova	Ukraine
Czech Republic	Montenegro	
Georgia	Poland	

Issuers must technically support MO/TO refund Transactions.

Issuers must technically support purchase with cash back Transactions. They must make individual authorization decisions and must not automatically decline authorization of purchase with cash back Transactions.

An Issuer must support partial amount preauthorization on Cards used at unattended petrol POS Terminals if the Issuer supports this transaction type when any other debit brand is used at unattended petrol POS Terminals.

Issuers in the countries listed below must support the Gaming Payment Transaction. Refer to Rule 9.4.8 of this chapter for more information.

Country Code	Country	Country Code	Country
020	Andorra	428	Latvia
040	Austria	442	Luxembourg
056	Belgium	470	Malta
100	Bulgaria	492	Monaco
196	Cyprus	528	Netherlands
203	Czech Republic	578	Norway
208	Denmark	642	Romania
233	Estonia	674	San Marino
250	France	703	Slovakia
280	Germany	705	Slovenia
292	Gibraltar	724	Spain
300	Greece	752	Sweden
348	Hungary	756	Switzerland
352	Iceland	792	Turkey

Country Code	Country	Country Code	Country
372	Ireland	826	United Kingdom
380	Italy		

Effective 11 April 2014, Issuers in the United Kingdom must support partial approvals and account balance responses.

Effective 19 April 2013, Issuers in Italy must:

1. support full and partial reversals for all prepaid Card account ranges; and
2. upon receiving a Reversal Request/0400 message or an Acquirer Reversal Advice/0420 message, release any hold placed on the Cardholder's account for the amount specified within 24 hours of matching the reversal message to the original authorization request message.

9.2.2 Acquirer Online POS Transactions

9.2.2.1 Required Transactions

1. Purchase.

   In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.2.1 (1) in part 1 of this rulebook, the following apply:

   The CVM must be either PIN or signature, except in the case of properly presented Maestro *PayPass* Transactions where no CVM is required. For *PayPass* Transactions that exceed the applicable ceiling limits, Cardholders are required to enter a PIN.

   No maximum Transaction amount applies to the purchase Transaction, except in the case of properly presented Maestro *PayPass* Transactions where ceiling limits apply. See Rule 9.13 in Part 1 of this rulebook for ceiling limit guidelines.

   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.

2. Reversal.

   In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.2.1 (2) 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.

Effective 17 April 2015, the Acquirer of a Merchant located in Italy identified under an MCC listed in the table below must support full and partial reversals performed at the POI and whenever, for technical reasons, the Acquirer is unable to communicate the authorization response to the Merchant, for all prepaid Card account ranges:

MCC	Description
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5542	Fuel Dispenser, Automated
5612	Women's Ready to Wear Stores
5691	Men's and Women's Clothing Stores
5732	Electronic Sales
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5999	Miscellaneous and Specialty Retail Stores

3. Partial approval.

Effective 11 April 2014, Acquirers must support partial approval for Merchants located in the United Kingdom and identified with MCC 5542 (Fuel Dispenser, Automated), or with an MCC listed in the table below with respect to Transactions conducted at attended POS Terminals.

MCC	Description
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5612	Women's Ready to Wear Stores
5691	Men's and Women's Clothing Stores
5732	Electronic Sales
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5999	Miscellaneous and Specialty Retail Stores

4. Balance response.
Effective 11 April 2014, Acquirers must support account balance response for Merchants located in the United Kingdom and identified with an MCC listed in the table below with respect to Transactions conducted with a prepaid Card at an attended POS Terminal.

MCC	Description
5310	Discount Stores
5311	Department Stores
5411	Grocery Stores, Supermarkets
5541	Service Stations (with or without Ancillary Services)
5612	Women's Ready to Wear Stores
5691	Men's and Women's Clothing Stores
5732	Electronic Sales
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5999	Miscellaneous and Specialty Retail Stores

9.2.2.2 Optional Online POS Transactions

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.2.2 in part 1 of this rulebook, the following apply:

'Scrip' and 'account selection' are not currently supported within the Europe Region.

'Refund' and 'cancel' functions are supported in place of 'correction'.

Acquirers and Merchants that support an optional Transaction type presented below must comply with the Rules in this section for each optional Transaction type that is supported.

Purchase with Cash Back Transactions

A Merchant must offer purchase with cash back Transactions to Cardholders if the Merchant offers this transaction type to cardholders of any other debit brand.

Merchant-approved Transactions

The Rules below replace the Rules on Merchant-approved Transactions set forth in part 1 of this rulebook.

In general:

Merchant-approved Transactions may optionally be processed under the following conditions:

1. This Transaction type must be used only when the POS Terminal has no online capability.
2. The Merchant must request authorization as soon as online capability is restored.
3. Merchant-approved Transactions may not be resubmitted after the Issuer has declined them. The Acquirer bears liability for Transactions that are declined by the Issuer.
4. Unauthorized Merchant-approved Transactions must not be cleared.

Emergency Fallback at Hybrid POS Terminals

Merchant-approved Transactions may be carried out at EMV-capable POS Terminals under the following conditions:

1. The POS Terminal has for a technical reason temporarily lost its online capability at the time of the Transaction,
2. The Card is an EMV Card,
3. The Cardholder's PIN is successfully verified offline by the chip (unless no CVM is required according to the Rules applicable to the particular Transaction type, for example, parking and tollways Transactions),
4. The POS Terminal recommends approval of the Transaction,
5. The chip on the Card declines offline authorization and instead seeks an online authorization.

In all presentment and authorization request messages, the Acquirer must provide the Application Authentication Cryptogram (AAC) in subelement 9 of data element (DE) 55 (Integrated Circuit Card [ICC] System-Related Data), which indicates that the chip has declined the terminal's offline authorization request.

In presentment messages only, the Acquirer must additionally provide a value of F (Offline Chip) in DE 22 (Point of Service Entry Mode), subfield 7 (Card Data Input Mode), which indicates that the terminal processed an offline chip transaction.

Emergency Fallback at Magnetic Stripe POS Terminals

Magnetic stripe Merchant-approved Transactions may be carried out at any POS Terminal under the following conditions:

1. The POS Terminal has for a technical reason temporarily lost its online capability at the time of the Transaction,
2. No specific CVM is required to be used for such Transactions, it being understood that only PIN provides protection in case of a chargeback under message reason code 4837.

Preauthorization

Preauthorization is permitted only at unattended petrol terminals (MCC 5524). Please refer to Rule 9.4.6 in this chapter.

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:

1. the Cardholder and Merchant must be informed;
2. there must be no record of a Transaction;
3. a reversal advice message must be reported to the Issuer.

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:

1. the Cardholder and Merchant must be informed;
2. the attempted Transaction must be recorded;
3. a reversal advice message must be reported to the Issuer with a response code.

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.

The refund Transaction may be used to return unused gambling value to the Cardholder, up to the amount of the original purchase. The Gaming Payment Transaction must be used to transfer gambling winnings to the Cardholder. Refer to Rule 9.4.8 of this chapter.

As the Issuer receives money, no Issuer authorization is required for a refund. Cardholders should be asked for proof of purchase (receipt etc.) showing that the original Transaction was undertaken using a Card as the payment method.

PIN verification is not supported or required for intra-European refund Transactions as these Transactions are submitted without authorization.

MO/TO refund Transactions may be processed to a Card without reading the magnetic stripe or chip on the Card.

A Transaction printout must be generated for a refund Transaction, with the exception of MO/TO refunds.

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.

Payment Transactions and MasterCard *MoneySend* Payment Transactions

Effective 19 April 2013, an Issuer in Italy must support, process, and provide a valid authorization response to each Payment Transaction and MasterCard *MoneySend* Payment Transaction authorization request received. Except with respect to nonreloadable prepaid Cards, an Issuer must not automatically decline Payment Transactions or MasterCard *MoneySend* Payment Transactions.

9.3 Terminal Transaction Types

9.3.1 Issuer Requirements

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.3.1 in part 1 of this rulebook, the following applies:

Issuers must technically support PIN-Based In-Branch Terminal Transactions.

Issuers in the United Kingdom must support and offer at ATMs in the United Kingdom available and ledger balance inquiry functionality to their Cardholders.

Issuers in Russia, Czech Republic, Romania, and Slovakia must support and offer balance inquiry functionality to their Cardholders.

Effective 15 November 2012, in addition to Issuers in Russia, Czech Republic, Romania, and Slovakia, Issuers in Albania, Armenia, Belarus, Bosnia, Kosovo, Macedonia, Moldova, Montenegro, and Serbia must support and offer balance inquiry functionality to their Cardholders.

9.3.1.1 Issuer—Optional Transactions

Transfers from one Account to another and Account selection are not currently supported within the Europe Region.

Issuers in countries in the Europe Region other than those listed in Rule 9.3.1 above are allowed to offer balance inquiry to their Cardholders.

9.3.2 Acquirer Requirements

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.3.2 in part 1 of this rulebook, the following apply:

Transfers from one Account to another and Account selection are not currently supported within the Europe Region.

Acquirers in the United Kingdom must support and offer available and ledger balance inquiry functionality on UK-issued cards at all of their Terminals.

Effective 15 November 2012, Acquirers in Armenia and Belarus must support and offer balance inquiry functionality at all of their Terminals.

Acquirers in Russia, Poland, Czech Republic, Hungary, Romania, Ukraine, Slovakia and Croatia must support and offer balance inquiry and PIN change functionality at all of their Terminals.

Effective 15 November 2012, in addition to Acquirers in Russia, Poland, Czech Republic, Hungary, Romania, Ukraine, Slovakia and Croatia, Acquirers in Albania, Bosnia, Kosovo, Macedonia, Moldova, Montenegro, and Serbia must support and offer balance inquiry and PIN change functionality at all of their Terminals.

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.

9.3.2.1 Acquirer—Optional Transactions

Acquirers may support PIN-based In-Branch Terminal Transactions at their option.

The purchase of Merchandise from no account specified is permitted in the Europe Region.

9.3.3 Terminal Edit Specifications

Acquirers must send all Transactions to the Interchange System without performing edits.

For chip Transactions, Acquirers must not perform additional edits (either at a Terminal, or Acquirer host level) other than those defined in the chip technical specifications.

9.3.3.1 Acceptance and Transaction Routing

The Acquirer must consult the Member Parameter Extract file to determine if a card value is accepted by the Interchange System.

Table 40 of the Member Parameter Extract links account ranges to acceptance brands. By comparing the Card value with the account ranges in table 40 the Acquirer can determine if the Card is valid for routing to the Interchange System.

9.4 Special Transaction Types

9.4.3 Processing Requirements—Transactions Performed on Board Planes, Trains, and Ships

The Rules set forth in part 1 of this rulebook are modified as shown below.

Refer to Rule 9.2.2.2 of this chapter for the Rules about processing Merchant-approved Transactions.

A Customer may additionally process magnetic stripe Transactions that arise from a POS Terminal that has no fixed location (for example, a POS Terminal aboard a plane, train, or ship) even if that POS Terminal does not have an online connection as provided below:

1. No specific CVM is required to be used for such Transactions, it being understood that only PIN provides protection in case of a chargeback under message reason code 4837.
2. Such Transactions may only be completed under the following MCCs:
   a. 5309 (Duty Free Stores);
   b. 4111 (Transportation—Suburban and Local Commuter Passenger, including Ferries); and
   c. 4112 (Passenger Railways)
3. The Merchant must request authorization as soon as online capability is available. Merchant-approved Transactions may not be resubmitted after the Issuer has declined them. Unauthorized Merchant-approved Transactions must not be cleared.

9.4.4 Processing Requirements—Tollway Transactions

The Rules set forth in part 1 of this rulebook are modified as shown below.

Refer to Rule 9.2.2.2 of this chapter for the Rules about processing Merchant-approved Transactions.

Magnetic stripe and chip Transactions may be completed at tollways as provided below:

1. The Merchant must obtain authorization online from the Issuer or, for magnetic stripe Transactions only, may process the Transaction according to the Merchant-approved Transaction rules.
2. No CVM is required to be used for the Transactions, it being understood that only PIN provides protection in case of a chargeback under message reason code 4837.
3. The Transactions must be identified with MCC 4784 (Bridge and Road Fees, Tools).
4. The Merchant may at its option maintain a negative file, provided this is done in a PCI-compliant manner.

Issuers of chip Cards must be able to authorize such Transactions even when the chip data in the authorization message indicates "CVM not successful."

9.4.5 Processing Requirements—Parking Garage Transactions

The Rules set forth in part 1 of this rulebook are modified as shown below.

Refer to Rule 9.2.2.2 of this chapter for the Rules about processing Merchant-approved Transactions.

Magnetic stripe and chip Transactions may be completed at parking garages as provided below:

1. The Merchant must obtain authorization online from the Issuer, or, for magnetic stripe Transactions only, may process the Transaction according to the Merchant-approved Transaction Rules;
2. For Transactions equal to or below EUR 50 (or the local currency equivalent), no CVM is required, it being understood that only PIN provides protection in case of a chargeback under message reason code 4837; and
3. Transactions must be identified with MCC 7523 (Automobile Parking Lots and Garages).

Issuers of chip Cards must be able to authorize such Transactions even when the chip data in the authorization message indicates "CVM not successful."

9.4.6 Processing Requirements—Unattended Petrol POS Terminals

The requirements set out below apply only at unattended POS Terminals at petrol stations and must not be used in any other acceptance environment. Such POS Terminals must be identified with MCC 5542.

Acquirers of Merchants that accept Cards at unattended POS Terminals at petrol stations must process Transactions as follows:

1. The Acquirer must submit a preauthorization message containing the maximum amount determined by the Acquirer or Merchant.
2. The Issuer's authorization response may be for the full amount of the preauthorization or for a lesser amount determined by the Issuer. The Transaction is guaranteed up to the amount authorized by the Issuer. Approval of a lesser amount is referred to as partial amount preauthorization. The Transaction is guaranteed up to the amount authorized by the Issuer.
3. The Acquirer must inform the Issuer of the final Transaction amount via an advice message, which must be sent to the Issuer within 20 minutes of the authorization response message.
4. The Issuer must send an advice acknowledgement upon receipt of the advice message. Issuers must be able to receive advice messages and return advice acknowledgements in the preauthorization environment.

The Issuer must post the Transaction to the Cardholder's Account on the basis of the advice message, rather than the preauthorization response.

Support for partial amount preauthorization (as defined in subparagraph 2. above) is mandatory for Issuers and Acquirers that support this transaction type for any other debit brand.

The Presentment/1240 must contain the final Transaction amount in DE 4.

Chip Transactions at Unattended Petrol POS Terminals

In addition to the requirements set out above, the following requirements apply to chip Transactions completed at unattended petrol POS Terminals.

Preauthorizations on Chip Cards must be processed in accordance with the chip technical specifications. Preauthorizations may be completed online or offline. Once a preauthorization has been approved, the process of clearing the subsequently completed Transaction is identical to the process following a magnetic stripe preauthorization.

9.4.7 Processing Requirements—Mail Order/Telephone Order (MO/TO) Transactions (UK, Ireland, Turkey, and France)

Acquirers in the **United Kingdom**, **Ireland**, and **France** that acquire intracountry MO/TO transactions under other debit brands must also acquire MO/TO Transactions under the Maestro brand.

Merchants located in European countries designated by the Corporation may at their option offer MO/TO Transactions on Cards issued in the same country.

Merchants in the United Kingdom, Ireland, Turkey, and France may offer this option.

The Rules for MO/TO Transactions are the same as those for face-to-face POS Transactions except that:

1. MO/TO Transactions must not be performed using Maestro *PayPass* contactless payment functionality or include purchase with cashback Transactions;
2. a MO/TO Transaction must have its own unique Cardholder Authority as described in Rule 9.4.7.2, except in the circumstances described in Rule 9.4.7.3;
3. manual key entry of the PAN is the normal method of performing a MO/TO transaction.
4. there is no Cardholder verification procedure;
5. a zero floor limit is applicable for all MO/TO Transactions;
6. if an Issuer's response to an authorization request is incorrectly supplied as call referral, this must be translated into a decline;
7. Merchants must collect and transmit CVC 2 for all MO/TO Purchase Transactions. In addition, AVS checking is mandatory at UK Merchants that deliver foreign currency or travelers' cheques. AVS checking is optional for all other MO/TO Transactions. The Rules and procedures for such checks are defined in Rules 9.4.7.4, 9.8.10 and 9.8.11 of this Chapter 17;
8. Merchants must not present the Transaction until the goods or services are ready to be dispatched.
9. the Merchant does not give the Cardholder the Transaction receipt or the goods and/or services upon completion of the Transaction; they are either:
    a. delivered to the Cardholder by a method chosen at the Merchant's discretion; or
    b. collected by the Cardholder.

9.4.7.2 Cardholder Authorities

1. For a Mail Order Transaction: a document signed by the Cardholder or a document which the Acquirer considers to be acceptable in lieu of a signed document (for example, an authority sent by facsimile transmission);
2. For a Telephone Order Transaction, either:
    a. instructions given over the telephone by the Cardholder to the Merchant, either to the Merchant's staff or to equipment operated by the Merchant (for example, an interactive voice system); or,
    b. instructions given over the telephone by means of a text message from the Cardholder to the Merchant, via equipment operated by the Merchant;

A Cardholder Authority must contain:

1. the following details shown on the Cardholder's card:

a. PAN;

b. Cardholder's name; and

c. expiry date.

2. the CVC 2 as positioned in a white panel adjacent to the signature panel;
3. the Cardholder's home address (including postcode);
4. Transaction amount (including postage and packaging);
5. for a Telephone Order Transaction, the date when the Cardholder gave her/his authority;
6. if goods/services are to be delivered:

   a. the delivery address; and

   b. if the goods/services are to be delivered to or collected by a third party, the third party's name.

9.4.7.3 Transactions Per Cardholder Authority

1. Except as described in paragraphs 2. and 3. below, a Merchant that has been given a Cardholder Authority must enter one purchase Transaction for the full amount specified in the Cardholder Authority.
2. If the Cardholder has ordered more than one item of goods/services but the Merchant is unable to fulfill the whole of the order immediately the Merchant is permitted to enter:

   a. a Transaction for an amount representing the price of those items that will be provided to the Cardholder immediately; and

   b. further Transactions representing the price of the remaining items as and when those items are provided to the Cardholder.

3. Provided the Cardholder gives his consent the Merchant may enter two or more Transactions whose combined total amount equals the amount specified in the Cardholder's Authority.

Merchants must not use the provisions in paragraphs 2. and 3. above, to establish recurring Transactions.

9.4.7.4 CVC 2/AVS Checks

The following applies where the Merchant carries out AVS checking and for CVC 2 checks.

1. The Cardholder authority must include the CVC 2 shown on the Cardholder's Card.
2. When entering the Transaction, the Merchant must key in:
   a. the CVC 2; and
   b. numeric data in the Cardholder's address and postcode.
3. Online authorization must be sought for the Transaction.
4. The Acquirer must attempt to send the authorization request to the Issuer accompanied by the data referred to in paragraph 2. above.

When the Issuer's response to the authorization request is Approve, the Issuer must accompany its response with an indication as to whether, for each of the CVC 2, the address numerics and the postcode numerics:

1. the data matches information held in its own records; or
2. the data does not match information held in its own records; or
3. the address numerics and postcode numeric have not been checked; or
4. the data has not been supplied.

When the Acquirer sends a response to the authorization request to the Merchant's POS Terminal, the message must include the Issuer's CVC 2 and AVS responses.

The Merchant:

1. ust not re-use the CVC 2; and
2. must not retain the CVC 2 in any manner for any purpose. The CVC 2 on a Cardholder authority for a Mail Order Transaction must be rendered unreadable prior to storage.

For more information about the Address Verification Service, refer to Rule 9.8.10 in this Chapter 17.

9.4.8 Gaming Payment Transactions

Gaming Payment Transactions are available in the Europe region only. The following rules apply to Gaming Payment Transactions:

- The Payment Transaction rules described in Rule 7.5 of this rulebook apply to Gaming Payment Transactions.

- The Gaming Payment Transaction may only be used to transfer winnings to the same Card that the cardholder used to place the bet or purchase value used or usable for gambling.
- The Gaming Payment Transaction must be properly identified in authorization and clearing messages using MCC 7995, a Transaction type value of 28, and a Payment Transaction program type value of C04.
- Electronic commerce Merchants that process Gaming Payment Transactions must be MasterCard *SecureCode*-enabled, and must seek Cardholder authentication during authorization of the Transaction in which the bet is placed or the value to be used for gambling is purchased.
- In countries where MO/TO Transactions are permitted, MO/TO Merchants may use the Gaming Payment Transaction to transfer winnings in accordance with all applicable rules.
- Merchants that process Gaming Payment Transactions may not participate in the Maestro Advance Registration Program.
- The Gaming Payment Transaction must not exceed EUR 50,000.
- Anti-Money-Laundering requirements:
  - The Acquirer must consider its Merchants that submit Gaming Payment Transactions as higher risk under its anti-money laundering compliance program.
  - In addition to any requirement under applicable local law or regulation, the Acquirer must satisfy the Corporation's requirement to design and implement processes to conduct enhanced due diligence reviews of Merchants that submit Gaming Payment Transactions.
  - The Acquirer must ensure that Merchants that submit Gaming Payment Transactions have appropriate controls in place to identify their own customers and block suspicious activities or Accounts.
  - The Acquirer must have robust procedures and ongoing controls in place to monitor Transactions conducted by Merchants that submit Gaming Payment Transactions and to detect and report any potentially suspicious activity.
- Gaming Payment Transactions may only be processed by Europe Region Acquirers in countries where such Transactions are not prohibited by applicable law and only to Cards issued in the following countries:

Country Code	Country	Country Code	Country
020	Andorra	428	Latvia
040	Austria	442	Luxembourg
056	Belgium	470	Malta
100	Bulgaria	492	Monaco

Country Code	Country	Country Code	Country
196	Cyprus	528	Netherlands
203	Czech Republic	578	Norway
208	Denmark	642	Romania
233	Estonia	674	San Marino
250	France	703	Slovakia
280	Germany	705	Slovenia
292	Gibraltar	724	Spain
300	Greece	752	Sweden
348	Hungary	756	Switzerland
352	Iceland	792	Turkey
372	Ireland	826	United Kingdom
380	Italy		

- Issuers in the above countries must support the Gaming Payment Transaction in authorization and clearing messages.
- Gaming Payment Transactions will not be authorized in MasterCard Stand-In or down options services. Authorization is entirely under the control of the Issuer.

9.4.9 Processing Requirements—Recurring Payments

A recurring payment Transaction is a payment made in connection with an agreement between a Cardholder and a Merchant whereby the Cardholder has authorized the Merchant to bill the Cardholder's Card account on a continued, periodic basis (such as monthly, quarterly, or annually) without a specified end date. Each payment may be for a variable or a fixed amount.

By way of example and not limitation, the following are Merchant categories that typically process recurring payment Transactions:

- MCC 4814 (Telecommunication Services including but not limited to prepaid phone services and recurring phone services)
- MCC 4816 (Computer Network/Information Services)
- MCC 4899 (Cable, Satellite, and Other Pay Television and Radio Services)
- MCC 4900 (Utilities—Electric, Gas, Heating Oil, Sanitary, Water)
- MCC 5192 (Books, Periodicals, and Newspapers)
- MCC 6300 (Insurance Sales, Underwriting, and Premiums)

Merchants are permitted to submit recurring payment Transactions only after they have been registered and received a Corporation-assigned Merchant ID and static AAV. The Corporation-assigned Merchant ID and static AAV must be used when submitting such Transactions, except for the initial Transaction in a recurring payment arrangement if this Transaction is completed face-to-face. For the face-to-face Transaction, PIN is required and static AAV must not be provided.

Each recurring payment Transaction must contain a value of 4 (Standing order/recurring transactions) in DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence) in the authorization request message.

Issuers should provide a Merchant advice code in DE 48, subelement 84 of the authorization response message when declining a recurring payment Transaction authorization request. Acquirers and Merchants should be able to receive and act on the Merchant advice code when present.

For recurring payment Transactions relating to a bill invoiced to the Cardholder, it is recommended that in the First Presentment/1240 message, the Merchant name in DE 43 subfield 1 be followed by a space, the word "BILL" or the local language equivalent, a space, and the bill reference number.

The following applies to intracountry recurring payment Transactions occurring within France, Hungary, Ireland, Poland, Romania, Ukraine, and the United Kingdom:

If a recurring payment Transaction authorization request is declined by the Issuer, the Acquirer must ensure that the Merchant resubmits the Transaction no more than once per day for a maximum of thirty-one (31) consecutive days until the Transaction is approved by the Issuer.

9.8 Authorizations

9.8.2 Transaction Routing

NOTE

A Rule on this topic appears in Section 17b, "Single European Payments Area Rules," of this rulebook.

9.8.5 Chip Transaction Routing

NOTE

A Rule on this topic appears in Section 17b, "Single European Payments Area Rules," of this rulebook.

9.8.7 Authorization Response Time

9.8.7.1 Issuer Response Time Requirements

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.8.7.1 in part 1 of this rulebook, the following applies:

An Issuer using the Dual Message System must respond to an ATM Authorization Request/0100 message within eighteen (18) seconds. If a response is not received within eighteen (18) seconds, a time-out message will be generated to the Acquirer or the Transaction will be authorized using the Stand-In Processing Service.

An Issuer using the Stand-In Processing Service must respond to a POS Authorization Request/0100 message originating from a Merchant located in the Netherlands within seven (7) seconds. If no response is received, the Stand-In Processing Service will be invoked after seven (7) seconds. Issuers that do not use the Stand-In Processing Service will have ten (10) seconds to reply; if a response is not received within ten (10) seconds, a time-out message will be sent to the Acquirer.

9.8.9 Offline Chip Authorizations

9.8.9.1 POS Terminal Transactions

Chip Transactions may be authorized offline, by the chip, for all POS Terminal Transactions below or equal to the applicable international floor limit unless the chip or POS Terminal determines that online authorization must be obtained for other reasons.

If an online authorization cannot be completed for technical reasons, the Transaction may be authorized offline by the chip, at the Issuer's discretion. For Transactions above the international floor limit, the Issuer is only liable if Issuer authorization has been obtained.

Offline authorization must be undertaken in accordance with the chip technical specifications.

9.8.9.2 Terminal Transactions

All Terminals must be connected 'online' to a host computer. The host computer must be directly or indirectly connected to the Dual Message System for authorization.

All Terminal Transactions must be authorized online to Issuer, whether the magnetic stripe or the chip is used to initiate the Transaction. Transactions may not be authorized offline by the chip in the event that an online authorization cannot be completed for technical reasons.

9.8.10 Address Verification Service—Intracountry Transactions in UK Only

Acquirer and Issuer participation in the Address Verification Service (AVS) is mandated for UK intracountry MO/TO Transactions.

9.8.10.1 Acquirer Requirements for AVS

UK Acquirers must register for AVS processing with the Corporation and meet the following requirements:

1. The Acquirer must transmit address information, when provided by the Merchant, to the Issuer in the Authorization Request/0100 message for MO/TO Intracountry Transactions;
2. The Acquirer must be able to receive the AVS response data from the Issuer contained in the Authorization Request Response/0110 message and forward it to the Merchant.

9.8.10.2 Issuer Requirements for AVS

UK Issuers must register for AVS processing with the Corporation and meet the following requirements:

1. The Issuer must be able to verify AVS data contained in the Authorization Request/0100 message for MO/TO Transactions;
2. The Issuer must transmit a valid AVS response code to the Acquirer in the Authorization Request/0110 message.

Issuers that fail to register for AVS processing, or that do not provide a valid response code to Acquirers, will not be eligible to charge back MO/TO Transactions using chargeback Message Reason Code 4837—No Cardholder Authorization, where AVS data was provided by the Acquirer.

9.8.10.3 AVS Response Codes

The following table describes the possible responses that an Acquirer may receive to a request for an AVS check.

Response Code	Description
A	Address matches, postal code does not.
N	Neither address nor postal code match.
R	Retry—system unable to process.
S	AVS currently not supported.
U	No data from issuer/authorization system.

9.8.11 CVC 2 Mismatches—Intracountry Transactions in UK, Ireland, and France Only

If an Issuer receives CVC 2 data in an authorization request and it is invalid, (for example, the CVC 2 Field is not blank and the data does not match the data held on the Issuer's records), the authorization request must be declined.

If an authorization request is approved when the CVC 2 data submitted is invalid, the Issuer cannot charge the Transaction back if it is subsequently found to be fraudulent.

9.9 Performance Standards

9.9.1 Issuer Standards

The following Rule replaces Chapter 9, "Processing Requirements," Rules 9.9.1.1 and 9.9.1.2, in part 1 of this rulebook:

9.9.1.1 Issuer Failure Rate (Substandard Performance)

An Issuer failure rate that exceeds one percent (1%) for POS or ATM Transactions for two months in any 6 month period is substandard performance. The Issuer failure rate will not apply to a Processor until:

1. After the fourth calendar month of operation; or
2. Upon processing five thousand (5,000) Transactions in a calendar month; whichever occurs first.

Issuers that have been designated as having substandard performance may be subject to noncompliance assessments and will be mandated to implement the Stand-In Processing Service. Chip Issuers mandated to implement the Stand-In Processing Service will also be required to register for M/Chip Cryptogram Validation in Stand-In.

9.13 Ceiling Limit Guidelines (Maestro *PayPass* POS Transactions)

In addition to Chapter 9, "Processing Requirements," Rule 9.13 in part 1 of this rulebook, the following applies:

If a Transaction exceeds the applicable ceiling limit, PIN must be used as the CVM.

NOTE

Maestro *PayPass* Transactions that exceed the applicable ceiling limit and have been verified by online PIN or through offline verification of a mobile PIN by a Mobile Payment Device will not have chargeback rights under Message Reason Code 4837. Refer to the *Chargeback Guide*, Appendix B for additional information.

9.14 Euro Conversion—Timing

Transactions submitted into the Interchange System that take place in countries that convert to the euro should be submitted in the euro.

To allow a grace period for exceptional cases, the Interchange System will not reject Transactions submitted in currencies that have been replaced by the euro within six (6) months after the transition period. Within this six (6)-month period, Issuers may not reject or chargeback Transactions submitted in currencies that the euro has replaced, solely on grounds that such Transactions have not been submitted in euro.

9.15 Clearing and Presentments

9.15.1 Clearing

Transactions must always to be cleared electronically using the Integrated Product Message (IPM) format.

Detailed clearing specifications are contained in the *IPM Clearing Formats* manual.

Transactions must be submitted into clearing within seven (7) calendar days of the Transaction date.

If the Acquirer does not submit an interregional Transaction into clearing within 120 days of the Transaction date, the Transaction will be rejected automatically by the Interchange System, and a credit adjustment for the Transaction amount will be processed to the Issuer by the Interchange System.

10.2 Settlement

In addition to the Rules in Chapter 10, "Settlement and Reconciliation," Rule 10.2 in part 1 of this rulebook the following apply:

As net settlement is the default procedure, if a Customer wishes to operate on a multilateral basis via the services available through the Corporation, it should be allowed to do so and may not be forced into bilateral agreements.

For further information about settlement, please refer to the *Settlement Manual*.

10.2.2 Assessment for Late Settlement

As described in the *Settlement Manual*, a Customer is not permitted to maintain a balance under zero on its account with the settlement bank. In order to remedy any debit position, every Customer is required to transfer on a daily basis to its settlement account the funds necessary to bring the account balance up to zero.

If the Customer does not comply with this requirement, the Corporation will assess the Customer daily based on the amount of the deficit. The assessment will be on the first day of failure to transfer funds in a timely manner and for each subsequent day on which funds are overdue.

"Assessments" in Chapter 1 of the *Settlement Manual* is modified as follows:

Customers are assessed according to the schedule in the billing manual applicable to them.

No assessment will be charged if the Customer's deficit is less than USD 2,000 per day.

This assessment will not apply if the settlement failure is the result of natural disaster, strike, local holidays, delay on the part of the settlement bank, or any event beyond the Customer's control.

10.2.4 Settlement Finality

The Corporation determines the net obligations of the participants in its payment system under its Rules and operating procedures. Customers' net obligations are calculated by the Corporation's proprietary small value clearing systems and are based upon accepted financial messages submitted by the participants to the Interchange System. Financial messages are considered irrevocable, by Customers, upon completion of the clearing system cutoff. However, in accordance with the Rules and operating procedures, Customers may submit a separate financial message to offset a previously submitted financial message.

The Corporation subsequently creates instructions, reflecting the Customers' end-of-day net obligations, which result in the assumption or discharge of payment obligations between Customers. These instructions are effected by Customers and the settlement agents of the Corporation. Settlement finality of the transfer order is determined by the rules of the national payment system in which the funds transfer is executed.

10.2.4.1 Cooperation with Government Authorities

Each Europe Region Customer agrees and acknowledges that, for the purposes of administering the Interchange System, the Corporation may from time to time co-operate (by sharing of information or otherwise) with:

1. the Financial Services Authority;

2. the Bank of England;
3. any relevant office holder (as defined in the UK SFD Regulations); and
4. any authority, body or person having responsibility for any matter arising out of, or connected with, the default of a Customer.

10.2.4.2 Provision of Information

For the purposes of the UK SFD Regulations, each Europe Region Customer must (except if such request is frivolous or vexatious) provide to any interested person who requests it, within 14 days of such request and upon payment by such a person of a reasonable charge:

1. details of the systems which are designated for the purposes of the Settlement Finality Directive in which such Customer participates; and
2. information about the main rules governing the functioning of such systems.

10.2.4.3 Notification of Winding Up Resolution or Trust Deed

For the purposes of the UK SFD Regulations, each Europe Region Customer must:

1. upon the passing of a creditor's voluntary winding up resolution (or analogous procedure in the jurisdiction of incorporation of such Customer) in respect of that Customer; or
2. upon a trust deed granted by the Customer becoming a protected trust deed.

notify the Corporation and the Bank of England that such a resolution (or analogous procedure) has been passed or that such a trust deed has become a protected trust deed, as the case may be.

10.7 Interchange and Service Fees

The following additional Rule applies in the Europe Region:

Acquirers must submit Transactions completed at Merchants with the interchange rate designator for the lowest fee tier applicable to them.

10.11 Customer Insolvency and Settlement Liability

In addition to the Rules in Chapter 10, "Settlement and Reconciliation," in part 1 of this rulebook, the following apply:

Customers must at all times comply with the policy presented in *MasterCard Customer Risk Management—A Quick Glance*.

The policy calls for the evaluation of a Customer's initial and continuing ability to avoid excessive risk to the other Customers Corporation. Within the framework of this policy, specific criteria have been established to determine the financial soundness of Customers and their Activities. Such criteria include both objective standards such as the measurement of capital adequacy and subjective standards, such as evaluating key management experience and ability and the manner in which such business is conducted.

If the Customer or applicant does not fulfill the criteria mentioned above, the granting or continuance of a License will be conditioned on compliance by the Customer with special conditions, within the framework of the policy. Examples of such special conditions are letters of credit, letters of guarantee or pledge agreements.

For an applicant, a protective arrangement will need to be in place before it can go live on Dual Message System.

If a Customer resists or excessively delays establishing a protective arrangement, the Corporation has the authority to collect the collateral it deems necessary through the settlement process in addition to the Customer's settlement volumes.

Unless circumstances are such that the Corporation, in its sole discretion, considers it necessary to collect the collateral without delay, it will not be collected until at least three weeks after the Customer is first notified in writing that it must comply with the initial request for collateral. Customers will be given seven calendar days' notice in writing before the collateral is actually collected.

The compliance of a Customer with the criteria relating to financial soundness will be re-examined from time to time.

10.11.1 Restrictions that Prevent the Settlement of Financial Obligations

If there are imposed laws or regulations, to which the Customer is subject, which prevent the Customer from settling its financial obligations in accordance with the Rules, the following shall apply:

1. the Customer must notify the Corporation immediately of the imposition of such laws or regulations; and
2. the Customer must immediately take all possible steps to prevent the creation of further financial obligations that it will be unable to meet. Examples of such steps would be the recalling of issued Cards and the issuance of Cards that do not cause such financial obligations.

10.11.2 Maintenance of System Liquidity

If the Corporation requires additional funds to maintain system liquidity and to meet the settlement obligations of failed Customers for which the Corporation guarantees Transactions, it may, upon two (2) working days' notice in writing, obtain the required funds from the other European Customers by debiting their settlement accounts. The funds will be collected by decreasing the Customers' gross daily settlement amounts of outgoing volumes by up to five per cent (5%) of the amount settled on the day of notification and by increasing Customers' gross daily amounts of incoming volumes by up to five per cent (5%) of the amount settled on the day of notification.

If necessary, collection will continue on the same basis on the days following the day of notification, for as long as needed to satisfy the settlement obligations of failed Customers and to ensure system liquidity. The Regional President or his designee will have responsibility for determining whether and/or when circumstances calling for application of this Rule exist.

The funds collected will be treated as advance payments on the sums that may be required from all Customers in the sharing out of loss. If the funds collected from a Customer exceed the amount ultimately charged to it in the final allocation, the excess will be returned to the Customer with interest payments based on the average overnight credit rate applicable to the currency as defined by central banks in the respective countries between the date(s) of collection of funds and the date of the final allocation.

If the funds collected from a Customer fall short of the amount charged to it in the final allocation, the Customer will pay the shortage to the Corporation with interest calculated in the same manner.

10.11.3 Loss Allocation Among Customers

Any losses incurred by the Corporation, or for which the Corporation may otherwise be responsible due to the failure of a Customer to perform its settlement obligations, will be apportioned among the European Customers. The apportionment of losses will be based on Customers' guaranteed issuing and acquiring volumes. The collection of the loss allocation will be undertaken by the Corporation as soon as practicable under the circumstances of the settlement losses and may be carried out over an extended period if required.

13.9 Merchant-approved Transactions

The Rules set forth in part 1 of this rulebook are modified as shown below.

The Issuer is liable for Merchant-approved Transactions that it has authorized. Its liability is the same as for online Transactions that it has authorized. The Acquirer requests authorization only once as such Transactions must not be resubmitted. Thus, the Issuer will either approve or decline the authorization only once.

13.13 Additional Liabilities

13.13.1 Unjust Enrichment

If a Customer has been unjustly enriched, due to an error relating to the Corporation, the amount with which it has been enriched will be deducted from it and reimbursed to the Customer or Customers who have suffered the corresponding loss.

13.13.2 Non-Customer Claims

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

13.13.3 Force Majeure

Neither the Corporation nor the Customer is liable for noncompliance with the Rules if the noncompliance is due to force majeure, for example: law or regulation, an order by a public authority, telecommunications or electricity disruption outside the control of the non-complying party, fire, water damage, natural catastrophe, impending or actual war, revolt, civil unrest, general or sectorial industrial action, blockade, boycott, general or sectorial lockout, sabotage or an act of terrorism.

Additional Regional Information

Europe Geographical Region

Refer to Appendix A, "Geographical Regions," in part 2 of this rulebook.

Technical Specifications

Refer to Appendix B, "Technical Specifications," in part 2 of this rulebook.

Maestro Merchant Operating Guidelines (MOG)

Refer to Appendix C, "Maestro Merchant Operating Guidelines," in part 2 of this rulebook.

Signage, Screen, and Receipt Text Displays

Refer to Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
1.7 Termination of License	A
2.3 Area of Use	A
3.4 Examination and Audits	A
3.6 Non-discrimination	A
3.7 Provision and Use of Information	A
3.8 Record Retention	A
3.21 Additional Obligations	A
3.22 Data Protection	A
4.2 Protection and Registration of the Marks	A
4.5 Display on Cards	B
4.6 Display of the Marks at POI Terminals	B
5.2.2 Program Approval	A
5.3.1 Standards for All Communications	B
5.4.3 A/CB Card Design—Partner's Identification	B
5.4.4 A/CB Card Design—Program Names	B
6.1 Eligibility	A
6.2 Card Standards and Specifications	A
6.2.3 Chip Card Standards	A
6.2.3.4 Chip Card and Chip Transaction Plans	C
6.4 PIN and Signature Requirements	A
6.9 Electronic Commerce	A
6.10 Selective Authorization	B
6.11 MasterCard *MoneySend* Payment Transaction	A
6.13 Issuer Responsibilities to Cardholders	B

Rule Number/Rule Title	Category
6.14 Fraud Reporting	A
6.16 Co-residing Applications	A
6.17 Additional Rules for Issuing	B
7.1 Acquirer Obligations and Activities	A
7.1.15 Information to Merchants—European Economic Area Only	B
7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only	A
7.4 Acquiring Electronic Commerce Transactions	A
7.5 Acquiring Payment Transactions	A
7.9 POS Terminal and Terminal Requirements	A
7.10 Hybrid POS Terminal and Hybrid Terminal Requirements	A
7.11 Additional Requirements for POS Terminals	A
7.12 Additional Requirements for ATMs	A
7.13 Additional Requirements for PIN-based In-Branch Terminals	A
7.14 POI Terminal Transaction Log	A
7.15 Requirements for Transaction Receipts	B
7.17 Connection to the Interchange System	A
7.18 Card Capture	A
7.20 Merchandise Transactions	B
7.23 ATM Access Fees	B
7.27 Identification of *PayPass* Transactions	A
8.4 PIN and Key Management Security Requirements	A
8.13 Signature-based Transactions	A
8.14 Audit Trail	A
8.15 Inspection of Customers	A
9.2 POS Transaction Types	A
9.3 Terminal Transaction Types	A
9.3.1 Issuer Requirements	B
9.3.2 Acquirer Requirements	B

Rule Number/Rule Title	Category
9.4.3 Processing Requirements—Transactions Performed on Board Planes, Trains, and Ships	C
9.4.4 Processing Requirements—Tollway Transactions	C
9.4.5 Processing Requirements—Parking Garage Transactions	C
9.4.6 Processing Requirements—Unattended Petrol POS Terminals	B
9.4.7 Processing Requirements—Mail Order/Telephone Order (MO/TO) Transactions (UK, Ireland, Turkey, and France)	C
9.4.8 Gaming Payment Transactions	B
9.4.9 Processing Requirements—Recurring Payments	B
9.8 Authorizations	A
9.9 Performance Standards	A
9.13 Ceiling Limit Guidelines (Maestro *PayPass* POS Transactions)	A
9.14 Euro Conversion—Timing	C
10.2 Settlement	A
13.9 Merchant-approved Transactions	A
13.13 Additional Liabilities	A

Section 17a UK Maestro Intracountry Rules

This section contains Rule variations or additional Rules applicable to the United Kingdom.

Overview

NOTE

These revised rules relating to UK Maestro became effective 13 May 2011.

Set forth below are the rule variations to part 1 and Chapter 17, "Europe Region" of the *Maestro Global Rules*, and additional rules for UK Intracountry Transactions. In most cases, this UK chapter supplements the Europe Region's rules and UK Intracountry participants must comply with the rules in part 2, Chapter 17, and the UK chapter of this rulebook, as applicable.

If a section in the UK chapter contains the full set of rules applicable to UK Intracountry participants, in place of the corresponding section in part 1 or Chapter 17, "Europe Region" of this rulebook, then this is clearly mentioned, and UK Intracountry participants are required to comply only with the rules in that UK section.

In all cases, UK Intracountry participants should refer to part 1 of this rulebook in the first instance.

The UK Maestro Intracountry rules govern Transactions performed with a Card bearing the Marks issued on an Account domiciled in the UK, Channel Islands or Isle of Man (the "Territory") at a Merchant whose business address is within any of these countries ("Intracountry Transactions"). For further information concerning "Area of Use," refer to Chapter 1 in part 1 of this rulebook, and Chapter 17, "Europe Region," in part 2 of this rulebook.

The rules contained in this Section 17a do not apply to ATM and PIN-Based In-Branch Terminal Transactions.

Definitions

The following UK section contains additional definitions or variations to the "Definitions" and the "Glossary" in part 1 of this rulebook, and Chapter 17, "Europe Region," in part 2.

Internet Stored Value Wallet

A virtual wallet that can be loaded and unloaded via electronic commerce Transactions.

Mail/Telephone Order (MO/TO) Merchant

A Merchant in which no face-to-face Transactions are performed.

Territory

The countries in which the UK Intracountry rules apply, which are the United Kingdom (that is, Great Britain and Northern Ireland), the Isle of Man and the Channel Islands. These countries are deemed to include:

- (providing the Merchant's address is within one of the countries) trains, ships and airplanes traveling to or from any one of them; and
- all UK armed forces' ships and bases where ever they may be located.

UKCA

UK Cards Association

6.2 Card Standards and Specifications

6.2.1 Encoding Standards

6.2.1.3 Primary Account Number (PAN)

In addition to the rules in Chapter 6, "Issuing," Rule 6.2.1.3 (1), paragraph 5 in part 1 of this rulebook, the following applies:

All UK Maestro Cards issued within the Territory must fall within the BIN range 675900 to 675999 and 676770 to 676774.

6.2.5 Signature Panel

In addition to the rules in Chapter 6, "Issuing," Rule 6.2.5 in part 1 of this rulebook, the following applies:

Issuers must indent print on the card the CVC 2 either on the signature panel or in a white panel adjacent to the signature panel.

6.3 Optional Card Security Features

Issuers may use the UKCA cheque guarantee hologram up to 30 June 2011. Cards issued after this date cannot carry this hologram.

7.1 Acquirer Obligations and Activities

7.1.2 Before Signing a Merchant

In addition to the rules in Chapter 7, "Acquiring," Rule 7.1.2, in part 1 of this rulebook, the following apply:

Before signing a Merchant Agreement with a potential Merchant, an Acquirer must check whether or not the potential Merchant, or any of its outlets, appears on the MATCH files. If an entry appears, any resulting contact with another Acquirer must be performed by the Acquirer itself (that is, must not be delegated to agents).

7.1.16 MATCH

Acquirers must refer and report to Merchant Alert to Control High-Risk Merchants (MATCH).

Refer to the *Security Rules and Procedures* manual for information about the standards and reason codes that must be supported.

7.9 POS Terminal and Terminal Requirements

7.9.8 Cardholder-Activated Terminals (CATs)

CATs must:

1. be configured so that the transaction amount is limited to the following maximum value, dependent upon the applicable Merchant Category:

MCC	Merchant Category	Maximum Transaction Amount* (£)
30xx–32xx	Airlines with Specific Merchant Category Codes	300
35xx–37xx	Hotels with Specific Merchant Category Codes	300
4111	Ferries	300
4112	Passenger Railways	300
4131	Bus Lines	300
4511	Air Carriers, Airlines – not elsewhere classified	300
5542	Automated Fuel Dispensers	60
7011	Lodging – Hotels, Motels, Resorts – not elsewhere classified	300
7523	Car Parks	130
7832	Motion Picture Theatres	300
7922	Theatrical Producers (except Motion Pictures), Ticket Agencies	300
–	Other Categories	50

* Authorization must be requested for the full transaction amount, with the exception of Automated Fuel Dispensers, where the authorization request must be for a nominal £1.

2. In the case of Automated Fuel Dispensers, where the maximum Transaction amount is £60

   a. check the limit for each Transaction;

   b. advise Cardholders of such a limit before the PIN is entered.

7.9.8.1 Smart Card Loading CAT Devices

At CATs that are Smart Card Loading Devices

1. the smart Cards to be loaded must:
   a. be issued
      i. by the Merchant that operates the device;
      ii. only to holders whose names and addresses are known to the Merchant;
   b. bear a means to verify the smart Card holder on each occasion that she or he uses the smart Card:
   c. not be capable of being used to obtain cash;
   d. not bear any detail of the smart card holder's Card(s);
2. if the smart Card has its own PIN, the Merchant must:
   a. discourage the holder from using the same PIN for her/his Card;
   b. not store details of the PIN with Card details;
3. the loading device may use stored details of a Card for Transactions providing they are derived from a Transaction in which the Card itself was used;
4. the Card Acceptor Name/Location Data provided in a Transaction Interchange File for a Transaction performed at a loading device must contain:
   a. the words "Value Load";
   b. the Merchant's name.

9.2 POS Transaction Types

9.2.2 Acquirer Online POS Transactions

9.2.2.2 Optional Online POS Transactions

Purchase with Cashback

The following replaces the rule in Chapter 9, "Processing Requirements," Rule 9.2.2.2 (2.b) paragraph 3 in part 1 of this rulebook

A maximum cashback amount of £100 must be observed.

9.4 Special Transaction Types

The Rules are supplemented or varied for Transactions performed at the following types of Merchant:

1. Internet Stored Value Wallet Load;
2. Telephone Pre-payments;
3. Transit Auto Top-Up Merchants.

Transactions must not be performed at the above special Merchant types using Maestro *PayPass*.

9.4.1 Processing Requirements—POS Unique Transaction Types

In addition to the rules in Chapter 9, "Processing Requirements", Rule 9.4.1 (4) in part 1 of this rulebook, the following applies:

4. Quasi Cash (MCC 6051—Merchant)

a. For a Mail Order/Telephone Order (MO/TO) Transaction for currency and/or travelers cheques that are to be delivered.

i. the Cardholder authority must include the Cardholder's telephone number;

ii. a name and address check or a CVC2/AVS check must be performed. Refer to Chapter 17, "Europe Region" for further information.

iii. authorization must be obtained;

iv. the total amount of such Transactions must not exceed £3,000 per Cardholder per day.

b. For electronic commerce Transactions for currency and/or travelers cheques that are to be delivered, the total amount of such Transactions must not exceed £3,000 per Cardholder per day.

c. Purchases of sterling are not permitted, except at Merchants on board ships that have no other banking facilities. At such Merchants if sterling is purchased;

i. secondary identification must take the form of a passport, full driving license, or Armed Forces I.D.;

ii. the amount of the Transaction must not exceed £500;

In addition to the rules in Chapter 9, "Processing Requirements", Rule 9.4.1 (5) in part 1 of this rulebook, the following applies:

5. Gambling Transactions (MCC 7995)

a. For Mail Order/Telephone Order Transactions Cardholder authorities must:

i. contain a Personal Registration Number given to the Cardholder by the Merchant as per the rules in this subsection paragraph 3. below, before the Cardholder performs the first Transaction at any of the Merchant's outlets;

ii. although the authority for a first Transaction at a Merchant must conform to normal UK Intracountry Maestro rules, authorities for subsequent Transactions need not include;

- Card's PAN;
- Cardholder's name;
- expiry date;
- Cardholder's home address;

b. Name and address checks are not permitted.

c. The following rules apply to the giving of Personal Registration Numbers:

i. A Merchant must not give a Cardholder a Personal Registration Number unless:

- it has obtained the Cardholder's name and address;
- a POS Terminal at one of its outlets has accepted the following details from the Cardholder's Card: PAN and expiry date;

ii. If the Cardholder uses a Card other than the Card whose details have been accepted by the Merchant's POS Terminal (for example, following the issue of a new Card):

- details of the other Card must also be accepted by a POS Terminal at one of the Merchant's outlets;
- a Personal Registration Number must be provided to the Cardholder for use with the other Card.

c. Authorization must be performed for every purchase and Purchase with Cashback Transaction and the Cardholder must be advised of the outcome before a bet is accepted

9.4.8 Gaming Payment Transaction

Face-to-face gambling Merchants may use the Gaming Payment Transaction to transfer winnings in accordance with all applicable rules. Gambling Merchants that are legally required to transfer winnings to the same Card that was used to place the bet or purchase gambling value must use the Gaming Payment Transaction for this purpose.

9.4.9 Internet Stored Value Wallets Load

1. The loading/unloading of Internet Stored Value Wallets is allowed by means of electronic commerce Transactions provided;

   a. such a wallet:

      i. has PIN/password entry to verify the account holder on each occasion that the account holder performs a load or unload;

      ii. is capable of being blocked by the Merchant to prevent loading.

   b. Stored Value Wallet password/PIN details are not stored with Card details;

   c. the wallet-holder is discouraged from using the same PIN for the Card and wallet account

2. Where electronic commerce Transactions are used to load/unload Stored Value Wallets:

   a. the Merchant must conform to the rules for electronic commerce Merchants

   b. a Transaction is permitted only if the details (i.e. PAN) have previously been registered with the Merchant;

   c. the Cardholder's instructions must be acknowledged by e-mail;

   d. wallets must only be unloaded using the Payment Transaction type and only on to the Card used for loading;

3. CVC2/AVS checks must be undertaken in some circumstances: refer to Chapter 17, "Europe Region" of this rulebook for further information.

9.4.10 Telephone Pre-payments (Mobile Phones and Unspecified Phones)

1. A Transaction is permitted only if the Card's details (i.e. PAN) have previously been registered with the Merchant for pre-payments as per the following rules:

   a. no more than two (2) Cards may be registered (per phone in the case of mobile phones);

   b. where registration is for mobile phone(s), no more than two (2) phones may be registered per Card;

   c. the Merchant must obtain and verify the Cardholder's name and home address by one of the following methods:

      i. obtaining from the Cardholder the address or details from the address and either:

- providing details from the address (for example, AVS data) to the Issuer for verification; or
- verifying the address/details against a utility bill and/or bank statement; or

ii. obtaining details from the address from the Issuer.

2. Authorization must be obtained for every purchase Transaction.
3. Transactions must be processed using Merchant Category Code 4814.
4. If a Transaction is charged back on grounds of fraudulent use:

a. the Acquirer must inform the Merchant;

b. the Merchant must:

i. if a mobile phone has been used, disconnect the phone(s) for which the Card is registered;

ii. if an unspecified phone has been used, not permit the Cardholder to make any more calls;

iii. cancel registration of the Card used to perform the Transaction;

iv. not re-register a Card with the same details.

9.4.11 Transit Auto Top-Up Payments

1. Cardholders issued with a pre-pay card from a transit company offering the auto top-up service may auto-top-up their cards with set amounts when the amount held on the card falls below an agreed level using their Maestro Card, under the conditions described below:
2. All cards must be registered for the service. This includes any cards new to the Cardholder subsequent to the initial registration and opt-in process;
3. A maximum of two (2) debit cards only may be registered per auto top-up card;
4. Any one debit card can be registered against a maximum of two (2) auto-top-up cards only;
5. Cardholders can register for this auto-top-up service via the Internet and formally opt-in by use of e-mail before this method of topping up their cards is enabled. When this service is offered via the Internet, some form of fraud screening must be undertaken. The initial Transaction, classed as e-commerce Transaction, must be supported using *SecureCode*. Subsequent Transactions will be classed as MO/TO and must be flagged accordingly. If any checks fail, the Transaction must not proceed;
6. MO/TO registration for this service is also permitted, whereby a cardholder contacts the call centre, is supplied with an authority form for completion, which includes name and address, card number, expiry date, top-up amount and signature. On receipt, the transit company telephones the customer to undertake a CVC2/AVS check. The registration is not progressed if the

Cardholder authority is not returned. Refer to Chapter 17, "Europe Region" of this rulebook for further information about CVC2/ AVS checking;

7. Cardholders can register for this service in a face-to-face environment. For POS Transactions, the initial Transaction must be conducted using the chip with no possibility of fallback. Subsequent Transactions may be undertaken as MO/TO and must be flagged accordingly;
8. All Transactions must be authorized and if approved Autoload is set up. In the case of a decline, the Cardholder will be contacted to verify payment details. If the outcome is unsatisfactory, the transit card must be hot-listed;
9. Standard liability applies to the initial Transaction and for subsequent Transactions, the Acquirer is liable in all cases;
10. Two outlet IDs are required: one for the initial Transaction and one for the subsequent transit auto top-up payments;
11. MCC 4111 must be used to allow accurate monitoring;
    a. The Acquirer must monitor chargeback volume/Transaction volumes in comparison to the Cardholder not present (CNP) average. The criteria should be;
        i. the number of chargebacks should not exceed 1% of total Auto Top-Up Transactions;
        ii. total gross fraud to turnover must not exceed scheme average CNP fraud to turnover;
        iii. total gross fraud to turnover must not exceed the average fraud to turnover ratio in MCC 4111 by 10% in any one month;
        iv. monitoring must be based on fraud Transaction data, therefore, be reviewed three months in arrears;
12. If a Transaction is disputed, the following procedures should be followed:
    a. Where a Transaction goes through after a Cardholder has cancelled his auto-top-up arrangement, compliance procedures may be initiated as documented in Appendix B of the Chargeback Guide; or
    b. Where a Transaction is fraudulent, chargeback code 4837 – "No Cardholder Authorization" should provide a right of chargeback;

All fraud may be charged back with the exception of the initial Transaction where standard liability applies.

Section 17b Single European Payments Area Rules

Overview

In the Single European Payments Area (SEPA), the Rules contained in this chapter modify or replace, as indicated, the Rules contained in part 1 and Chapter 17 of this rulebook.

The geographic scope of SEPA includes the following countries and territories:

Andorra	Latvia
Austria	Liechtenstein
Belgium	Lithuania
Bulgaria	Luxembourg
Channel Islands	Malta
Cyprus	Monaco
Czech Republic	Netherlands
Denmark	Norway
Estonia	Poland
Finland	Portugal
France	Romania
Germany	San Marino
Gibraltar	Slovakia
Greece	Slovenia
Hungary	Spain
Iceland	Sweden
Ireland	Switzerland
Isle of Man	United Kingdom
Italy	Vatican City

2.2 License Application

2.2.1 Single European Payment Area License

The following additional rules apply within SEPA:

Any entity that is eligible to become a Customer in one of the SEPA countries may request a SEPA License.

The Standards applicable to other Licenses also apply to SEPA Licenses, unless otherwise provided.

The SEPA License may be granted to Principals or Affiliates. The holder of a SEPA Principal License may sponsor Affiliates in one or more SEPA countries. The Affiliates may receive either a SEPA Affiliate License or a standard Affiliate License for the Marks.

If a SEPA License is held by a Customer that will undertake activities in one or more SEPA countries via separate legal entities, the separate legal entities must also sign Licenses.

The SEPA License may cover all of the countries in SEPA. If the SEPA License will cover both Switzerland and an EEA country, any Customer legal entity or SEPA Licensee that will be active both in Switzerland and in an EEA country must be regulated both in Switzerland and in an EEA country. The holder of a SEPA License must meet all local legal requirements in each country in which it intends to undertake activities.

The Customer is assigned a separate ICA for each SEPA country in which it is active, must use that ICA only for its Activity in that country, and must not undertake Activity in that country before the relevant ICA has been implemented.

The Customer is assigned a separate BIN or BIN range for each SEPA country in which it is active, must use that BIN or BIN range only for its Activity in that country, and must not undertake Activity in the country before the relevant BIN or BIN range has been implemented. For Card issuance, different ranges within a BIN may be linked to ICAs assigned for different SEPA countries.

With regard to Intracountry Transactions, the holder of a SEPA License must respect the applicable intracountry rules and fees.

3.6 Non-discrimination

In addition to Rule 3.6 of Chapter 17, the following Rule applies within SEPA:

A Customer must not, directly or indirectly, prevent or discriminate against the use of Maestro as a brand for Intracountry or Intra-SEPA Transactions.

By way of example but not limitation:

- a single certification must be valid for both intracountry and intra-SEPA use of the Maestro payment application at the POI Terminal;
- the prevalence of any particular chip-based payment application at POI Terminal or Acquirer system level must not be mandated or implemented;
- if the Maestro payment application is supported by both the Card and the POI Terminal, its use must not be blocked or impaired by technical or other means;
- if the Maestro payment application is supported by both the Card and the POI Terminal, the Cardholder must be given the opportunity to complete the Transaction with the Maestro payment application, in an EMV environment and in all other cases where the POI Terminal is technically capable of providing that choice to the Cardholder. In an EMV environment, if the Cardholder is not able to choose a payment application, the priority order defined by the Issuer in the chip must be respected.
- Neither the Cardholder's chosen payment application nor the Issuer's priority order may be disregarded or overridden by technical or other means.

4.5 Display on Cards

In addition, to Rule 4.5 of Chapter 17, the following Rule applies within SEPA:

Only the marks of payment schemes that are SCF-compliant may co-reside on Cards with the Marks.

NOTE

This Rule does not apply to Cards issued in the Netherlands until 2013.

6.2 Card Standards and Specifications

6.2.2 Embossing and Engraving Standards

The following Rule replaces Rule 6.2.2 (5) in part 1 of this rulebook:

5. Cards, except prepaid Cards, issued or re-issued after 1 April 2011 or following depletion of all Card stock in an Issuer's possession as of that date must bear the PAN on the front or back of the Card. It is strongly recommended that prepaid Cards bear the PAN on the front or back of the Card.

6.2.3 Chip Card Standards

In addition to Rule 6.2.3 of Chapter 17, the following Rule applies within SEPA:

Effective 1 October 2010, an Issuer of Cards that do not support both magnetic stripe and EMV chip technology must have an EMV migration project registered with MasterCard Customer Implementation Services.

Effective 1 January 2011, Cards must support both magnetic stripe and EMV chip technology. As an exception to the preceding rule, nonreloadable prepaid cards are not required to support EMV chip technology.

6.4 PIN and Signature Requirements

6.4.3 Use of PIN or Signature

In addition to Rule 6.4.3 of Chapter 17, the following rule applies within SEPA:

Intra-SEPA Transactions must be completed using PIN as the CVM.

7.10 Hybrid POS Terminal and Hybrid Terminal Requirements

In addition to Rule 7.10 of Chapter 17, the following Rule applies within SEPA:

Effective 1 October 2010, an Acquirer with any Terminals or POS Terminals deployed that do not support both magnetic stripe and EMV chip technology must have an EMV migration project registered with MasterCard Customer Implementation Services.

Effective 1 January 2011, POS Terminals and Terminals must support both magnetic stripe and EMV chip technology.

NOTE

POS Terminals in the Netherlands are not required to support EMV chip technology until 2013. An EMV migration plan for such POS Terminals is not required until 1 October 2012.

7.17 Connection to Interchange System

Each Participant must at all times accept all Cards at all ATMs owned or established by that Participant (including its parents, subsidiaries, affiliates, and sponsored entities) if it accepts cards issued under other acceptance brands at those ATMs.

9.8 Authorizations

9.8.2 Transaction Routing

Rule 9.8.2 in part 1 of this rulebook does not apply to intra-SEPA Transactions.

9.8.5 Chip Transaction Routing

Rule 9.8.5 in part 1 of this rulebook does not apply to Intra-SEPA Transactions.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
2.2 License Application	A
3.6 Non-discrimination	A
4.5 Display on Cards	B
6.2 Card Standards and Specifications	A
7.10 Hybrid POS Terminal and Hybrid Terminal Requirements	A
7.17 Connection to Interchange System	A

Chapter 18 Latin America and the Caribbean Region

This chapter contains Rule variations or additional Rules applicable to the Latin America and the Caribbean Region.

Overview

Set forth below are the Rule variations to the *Maestro Global Rules* and additional Rules for the Latin America and the Caribbean Region. In most cases, the Latin America and the Caribbean chapter supplements part 1 of this rulebook and Latin America and the Caribbean Customers must comply with the Rules in both part 1 and Chapter 18, "Latin America and the Caribbean Region," of this rulebook.

If a subsection in the Latin America and the Caribbean regional chapter contains the full set of Rules applicable to Latin America and the Caribbean Customers, in place of the corresponding chapter in part 1 of this rulebook, then this is clearly mentioned, and Latin America and the Caribbean Customers are required to comply only with the Rules in that Latin America and the Caribbean chapter.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

Definitions

In addition to the defined terms in the "Definitions," chapter in part 1 of this rulebook, the following apply:

Contactless Magnetic Stripe Transaction

In Brazil, a Transaction initiated by a Cardholder with a Card issued in Brazil at a Merchant located in Brazil, and which contains a value of 91 in Data Element (DE) 22 (Point of Service Entry Mode), subfield 1 (POS Terminal PAN Entry Mode), data field position 1–2 and a value of 3 or 4 in DE 61 (Point of Service [POS] Data), subfield 11 (POS Card Data Terminal Input Capability Indicator).

License, Licensed

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

Maestro *PayPass*

Maestro *PayPass* is a contactless payment functionality that uses radio frequency ("RF") technology to exchange Transaction data between a Chip Card, an Access Device, or a Mobile Payment Device, and a RF-enabled POS Terminal that bears the Maestro *PayPass* logo.

Marks

In Brazil, the term "Marks" means the MasterCard and Maestro names, logos, trade names, logotypes, trademarks, service marks, trade designations, and other designations, symbols, and marks that MasterCard International Inc., MasterCard International Incorporated and/or their affiliates or subsidiaries own, manage, license, or otherwise Control and make available for use by Customers and other authorized entities in accordance with a License. The MasterCard Mark must be accompanied by the proprietary "débito" graphic identifier on all Cards in accordance with the Identity Standards. A "Mark" means anyone of the Marks.

1.7 Termination of License

1.7.4 Liabilities and Obligations Following Termination

The following replaces Chapter 1, "Participation," Rule 1.7.4 (1) and (6) in part 1 of this rulebook.

Subject to the limitations set forth in the Rules, a terminated Customer may continue to assert any right accorded a Customer set forth in the Rules, and remain libel as a Customer to the Corporation and to its Customers for any matter occurring before the termination of its License.

4.1 Right to Use the Marks

In addition to the Rules in Chapter 4, "Marks," Rule 4.1, in part 1 of this rulebook, the following applies:

In Brazil, effective 1 January 2011, Customers that allow any of their Cardbases access to the Corporation must issue Card in compliance with the MasterCard "débito" Identity Standards and must be in full compliance by 1 February 2016.

In addition, when Customers use the MasterCard Mark accompanied by the proprietary "débito" graphic identifier, it must be as a stand-alone, domestic-use-only brand in compliance with the Identity Standards.

4.2 Protection and Registration of the Marks

In addition to the Rules in Chapter 4, "Marks," Rule 4.2, in part 1 of this rulebook, the following applies:

In Brazil, Customers must comply with the requirements set forth in Chapter 4, Trademarks and Service Marks, of the *MasterCard Rules* with regard to use of the MasterCard Marks.

The following applies to Cards issued in Puerto Rico and the U.S. Virgin Islands:

No use of a Mark may be made on or in connection with any card, device or other application associated with a payment service that the Corporation deems to be competitive with any Activity except as set forth in this chapter.

4.5 Display on Cards

In Brazil, the following Rules replace the second paragraph and fourth paragraph of Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook.

The Marks may be placed on cards in combination with other local/international ATM marks. The Marks may co-reside on a MasterCard card in the context of a multi-account card program. Customers must not place local/regional POS debit marks on Cards bearing the Marks and must be in full compliance with the requirements set forth in Rule 4.2.12, Use of Competing Marks on Card, of the *MasterCard Rules* as that provision may be amended from time to time.

The Marks may not be placed on any debit card that does not qualify as a Card.

In Puerto Rico and the U.S. Virgin Islands, the following replaces the second paragraph of Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook:

The Marks may be placed on a card in combination with any other local/regional/international POS debit mark and/or local/international ATM mark. In the event that a card has an international POS debit mark on the card front, and the card has a Maestro payment application:

1. if any other POS debit mark appears on the card back, the Marks must be displayed on the card back; or
2. if no other POS debit mark appears on the card back, the Marks are not required to appear on the card back.

A card must not include any visible indication communicating that acceptance or use of the Mark or the Maestro payment application is limited, geographically or otherwise.

The fifth paragraph of Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook in which Customers are prohibited from placing any other Competing EFT POS Network debit marks on their participating Cards does not apply to Cards issued in Puerto Rico or the U.S. Virgin Islands.

5.3 A/CB Communication Standards

5.3.1 Standard for All Communications

The following replaces the first and second paragraphs of Chapter 5, "Special Issuer Programs," Rule 5.3.1 in part 1 of this rulebook:

In Brazil, all solicitations, applications, advertisements, disclosures, and other material and information regarding any A/CB program (collectively for the purposes of this rules chapter only, "Solicitations") must refer prominently to the offering as a "MasterCard débito Card" and may not position the offering as something other than a Card. The A/CB brand name or logo may not be positioned as adding superior utility to the Card.

Any Solicitation regarding any MasterCard "débito" A/CB program must prominently and integrally feature the MasterCard Mark accompanied by the "débito" identifier and must identify the Issuer.

6.2 Card Standards and Specifications

6.2.5 Signature Panel

The following replaces Rule 6.2.5 of Chapter 6, "Issuing," in part 1 of this rulebook:

In Brazil, no signature panel or laser engraved signature is required on Cards bearing the MasterCard Mark accompanied by the proprietary "débito" graphic identifier. However, if a signature panel is used, it must be the authorized MasterCard signature panel in compliance with the Identity Standards.

6.3 Optional Card Security Features

The following replaces Rule 6.3 of Chapter 6, "Issuing," in part 1 of this rulebook:

In Brazil, Issuers must comply with the security features for Cards bearing the MasterCard Mark accompanied by the proprietary "débito" graphic identifier as set forth in the Identity Standards.

6.4 PIN and Signature Requirements

In addition to the Rules in Chapter 6, "Issuing," Rule 6.4 in part 1 of this rulebook, the following applies in Brazil:

The Cardholder must be verified by a PIN for any Maestro *PayPass* Transaction or Contactless Magnetic Stripe Transaction initiated with a Card issued in Brazil that exceeds the Maestro *PayPass* Transaction amount ceiling limit.

A CVM is not required for a Contactless Magnetic Stripe Transaction that is less than or equal to BRL 50.

6.4.2 Use of the PIN

6.4.2.1 Chip Cards

In addition to the Rules in Chapter 6, "Issuing," Rule 6.4.2.1 in part 1 of this rulebook, the following applies in Brazil:

4. The Chip Card must support online PIN verification as the CVM for any Maestro *PayPass* Transaction or Contactless Magnetic Stripe Transaction initiated with a Card issued in Brazil that exceeds the Maestro *PayPass* Transaction amount ceiling limit.

6.4.3 Use of PIN or Signature

In addition to the Rules in Chapter 6, "Issuing," Rule 6.4.3 in part 1 of this rulebook, the following applies in Brazil:

A CVM is not required for a Contactless Magnetic Stripe Transaction that is less than or equal to BRL 50.

6.10 Selective Authorization

In addition to the rules in Chapter 6, "Issuing," Rule 6.10, in part 1 of this rulebook, the following applies:

In Brazil, without the express written approval of the Corporation, a Customer may not launch or maintain a Card Program using the MasterCard Mark accompanied by the "débito" identifier for the purpose of selectively authorizing Transactions arising from use of Program Cards at only a subset of MasterCard débito acceptance locations. A Customer is not prohibited from authorizing or declining individual Transactions based on:

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

7.1 Acquirer Obligations and Activities

7.1.1 Signing a Merchant—POS and Electronic Commerce Only

7.1.1.1 The Merchant Agreement

In addition to the rules in Chapter 7, "Acquiring," Rule 7.1.1.1, in part 1 of this rulebook, the following applies:

In Brazil, Customers must comply with the requirements set forth in Chapter 4, Trademarks and Service Marks, of the *MasterCard Rules* with regard to use of the MasterCard Marks.

7.4 Acquiring Electronic Commerce Transactions

7.4.1 Acquirer Responsibilities: Electronic Commerce Transactions

The following replaces Rule 7.4.1 (1) of Chapter 7, "Acquiring," in part 1 of this rulebook:

In Brazil, Merchant sites must not display the MasterCard Mark accompanied by the "débito" identifier.

7.11 Additional Requirements for POS Terminals

7.11.1 Additional Requirements for Hybrid POS Terminals

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.11.1 in part 1 of this rulebook, the following apply in Brazil:

3. A POS Terminal in Brazil must support online PIN as the CVM for any Maestro *PayPass* Transaction or Contactless Magnetic Stripe Transaction initiated with a Card issued in Brazil that exceeds the Maestro *PayPass* Transaction amount ceiling limit.

7.17 Connection to the Interchange System

7.17.1 ATM Connection to the Interchange System

The following replaces paragraph 2 of Chapter 7, "Acquiring," Rule 7.17.1 in part 1 of this rulebook:

Customers that acquire Transactions must make available for connection to the Interchange System at least seventy-five percent (75%) of their eligible ATMs within one year (1) of the approval of its application for a License.

7.17.2 POS Terminal Connection to the Interchange System

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.17 in part 1 of this rulebook, the following applies:

Customers that acquire Transactions must make available for connection to the Interchange System at least seventy-five percent (75%) of their eligible POS Terminals within one (1) year of the approval of its application for a License.

7.18 Card Capture

7.18.1 POS Transactions

In addition to the second paragraph of Chapter 7, "Acquiring," Rule 7.18.1 in part 1 of this rulebook, the following applies:

Card Capture is not supported for intraregional POS Transactions.

7.23 ATM Access Fees

7.23.1 Domestic Transactions

The following replaces Chapter 7, "Acquiring," Rule 7.23.1, paragraph 1 in part 1 of this rulebook:

Upon complying with the ATM Access Fee notification requirements of the Rules, Acquirers in the Latin American and the Caribbean Region countries listed below may assess an ATM Access Fee on an intracountry Transaction so long as the Acquirer applies the ATM Access Fee in a consistent and nondiscriminatory fashion.

For the purposes of this Rule 7.23.1, ATM Access Fees shall mean a fee charged by an Acquirer in connection with any financial Transaction initiated at that Acquirer's ATM with a Card, which fee, is added to the amount of the Transaction transmitted to the Issuer. Further, an intracountry Transaction shall mean a Transaction initiated with a Card that was issued in the same country in which the ATM Transaction took place and that Transaction occurred in any of the following Latin American and the Caribbean Region countries:

Argentina	Brazil
Chile	Colombia

Ecuador	Mexico
Panama	Peru
Puerto Rico	Venezuela

7.23.1.1 Transaction Field Specifications

At the time of each Transaction on which an ATM Access Fee is imposed, the Acquirer of such Transaction must transmit the amount of the ATM Access Fee in the field specified in the *Single Message System Specifications* manual.

7.23.1.2 Non-Discrimination Regarding ATM Access Fees

An Acquirer must not charge an ATM Access Fee in connection with a Transaction that is greater than the amount of any ATM access fee charged by that Acquirer in connection with the transactions of any other network accepted at that Terminal.

7.23.1.3 Notification of ATM Access Fee

An Acquirer that is an Affiliate and that plans to newly impose an ATM Access Fee must notify its Sponsoring Principal, in writing, of its intent to do so prior to the planned first imposition of such ATM Access Fee by the Acquirer.

The Principal must update the Location Administration Tool (LAT) (formerly ATM directory/ATM Locator) regarding its or its Affiliates' imposition of ATM Access Fees.

7.23.1.4 Cancellation of Transaction

Any Acquirer that plans to add an ATM Access Fee must notify the Cardholder with a screen display that states the ATM Access Fee policy and provides the Cardholder with an option to cancel the requested Transaction.

7.23.1.5 Terminal Signage, Screen Display, and Transaction Record Requirements

An Acquirer that plans to newly impose an ATM Access Fee on a Transaction must submit proposed Terminal screen display and receipt copy that meets the requirements of the Rules to its Sponsoring Principal in writing for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook).

In addition, if the Acquirer displays Terminal signage, the Acquirer must submit proposed Terminal signage copy that meets the requirements of the Rules to its Sponsoring Principal in writing for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen and Receipt Text Displays," in part 2 of this rulebook).

The Sponsoring Principal has the obligation to determine the acceptability of any new or changes to previously approved Terminal signage, screen display, and receipt copy. In cases of conflict between an Affiliate and its Sponsoring Principal, the Corporation has the sole right to determine the acceptability of any and all Terminal signage, screen display, and receipt copy.

7.23.1.5.1 Additional Requirements for Terminal Signage

An Acquirer that plans to newly impose an ATM Access Fee on a Transaction may optionally display signage that is clearly visible to Cardholders on or near all Terminals at which ATM Access Fees apply.

The minimum requirement for ATM Access Fee Terminal signage text is wording that clearly states:

1. the name of the ATM Owner and Principal;
2. that the Transaction may be subject to an ATM Access Fee that will be deducted from the Cardholder's Account in addition to any Issuer fees;
3. the amount of, calculation method of, or Corporation-approved generic signage regarding the ATM Access Fee;
4. that the ATM Access Fee is assessed by the Acquirer instead of the Issuer; and
5. that the ATM Access Fee is assessed on intracountry Transactions only.

The minimum requirements for Terminal signage (physical characteristics) are as follows:

1. the signage must bear the heading "Fee Notice";
2. the size of the Terminal signage must be a minimum of four (4) inches in height by four (4) inches in width;
3. the text must be clearly visible to all. It is recommended that the text be a minimum of fourteen (14) point type;
4. the heading must be clearly visible to all. It is recommended that the text be a minimum of eighteen (18) point type.

A model for Terminal signage regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.1.5.2 Additional Requirements for Terminal Screen Display

An Acquirer that plans to newly impose an ATM Access Fee on a Transaction must present a screen display message that is clearly visible to Cardholders on all Terminals at which ATM Access Fees apply. If the Cardholder is given the option of choosing a preferred language in which to conduct the Transaction, the screen display message concerning ATM Access Fees must be presented to the Cardholder in that chosen language.

If an Acquirer displays the Corporation-approved generic ATM Access Fee signage, the Acquirer must include the amount of the ATM Access Fee as part of the Terminal screen display.

A model for the Terminal screen display regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.23.1.5.3 Additional Requirements for Transaction Records

An Acquirer that adds an ATM Access Fee on a Transaction must make available to the Cardholder on its Terminal receipt the ATM Access Fee information required by this Rule 7.23.1.5.3, in addition to any other information the Acquirer elects or is required to provide.

The minimum requirements for the Terminal receipt are:

1. a statement of the amount disbursed to the Cardholder;
2. a statement of the ATM Access Fee amount with language clearly indicating it is a fee imposed by the Acquirer;
3. a separate statement of the combined amount of the ATM Access Fee and the disbursed amount, with language clearly indicating that this amount will be deducted from the Cardholder's Account.

A model for Terminal receipt text regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.26 Discounts or Other Benefits at POS Terminals

A Card may access a discount or other benefit applied at a POS location, and the Merchant may promote such discount or other benefit at the POS location, provided such promotion does not disparage other Card programs.

9.2 POS Transaction Types

9.2.1 Issuer Online POS Transactions

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.2.1 in part 1 of this rulebook, the following applies:

11. balance inquiry

9.2.2 Acquirer Online POS Transactions

9.2.2.1 Required Transactions

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.2.1 (1) in part 1 of this rulebook, the following applies in Brazil:

1. Purchase

For each Maestro *PayPass* Transaction and Contactless Magnetic Stripe Transaction conducted in Brazil with a Card issued in Brazil that exceeds the Maestro *PayPass* Transaction amount ceiling limit, the Cardholder must enter a PIN.

A CVM is not required for a Contactless Magnetic Stripe Transaction that is less than or equal to BRL 50.

See Rule 9.13 in Part 1 of this rulebook for Transaction amount ceiling limit guidelines.

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.2.1 in part 1 of this rulebook, the following applies:

5. cancel

Acquirers and Merchants must ensure that each POS Terminal supports the electronic processing of the cancel Transaction.

9.2.2.2 Optional Online POS Transactions

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.2.2 (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.

9.8 Authorizations

9.8.2 Terminal Transaction Routing

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.8.2 in part 1 of this rulebook, the following applies:

All Transactions must be routed to the Interchange System for authorization.

For the avoidance of doubt, Rule 9.8.2 of Chapter 9, "Processing Requirements" of this rulebook does not inhibit a Merchant's ability to direct the routing of a transaction conducted in American Samoa, Guam, or Northern Mariana Islands with a Card that is issued in the United States Region, American Samoa, Guam, Northern Mariana Islands, Puerto Rico, or U.S. Virgin Islands to any debit payment network enabled on the Card.

9.8.13 CVC 3 Verification—Latin America and the Caribbean Region Only

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.8 in part 1 of this rulebook, the following applies in Brazil:

For each Contactless Magnetic Stripe Transaction, the Issuer must verify the CVC 3 value in the authorization request and provide the result in the response message.

9.13 Ceiling Limit Guidelines (Maestro *PayPass* POS Transactions)

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.13 in part 1 of this rulebook, the following applies in Brazil:

If a Transaction initiated with a Card issued in Brazil exceeds the applicable Transaction amount ceiling limit, online PIN must be used as the CVM.

NOTE

Maestro *PayPass* Transactions and Contactless Magnetic Stripe Transactions that exceed the applicable ceiling limit and have been verified by online PIN will not have chargeback rights under Message Reason Code 77. Refer to Chapter 4 of the *Chargeback Guide* for additional information.

11.2 Exception Transaction Types

11.2.1 POS Transactions

In addition to the Rules in Chapter 11, "Exception Item Processing," Rule .1 in part 1 of this rulebook, the following applies:

Customers are required to support the arbitration chargeback Transaction type.

11.8 Interchange Fees for Exception Transactions

In addition to the Rules in Chapter 11, "Exception Item Processing," Rule 11.8 in part 1 of this rulebook, the following applies:

Interchange fees associated with a Transaction will be reimbursed or reapplied as appropriate for the exception item being submitted. For example, a chargeback will cause the interchange fee to flow back to the Acquirer for a POS Transaction, and back to the Issuer for an ATM Transaction.

Percentage based interchange fees will be recalculated appropriately for exception items involving partial amounts.

13.12 Indemnity and Limitation of Liability

13.12.1 Indemnification against Losses

In addition to the Rules in Chapter 13, "Liabilities and Indemnification," Rule 13.12. in part 1 of this rulebook, the following apply:

Each Principal is responsible for and must indemnify and hold harmless the Corporation against losses, costs, expenses, liabilities and the like that the Corporation incurs, or for which the Corporation may otherwise be responsible, due to the failure of a Customer to perform its Customer obligations. Any losses that the Corporation incurs, or for which the Corporation may otherwise be responsible due to the failure of a Customer to perform its Customer obligations, will be allocated to the Principals. The allocation will be determined by the Corporation or in accordance with expense allocation practices in effect at that time, whether regional, global, operational, or any other.

The Corporation will determine the timing of the collection, which will be as immediate as is practicable, but may be carried out over an extended period if deemed necessary or appropriate.

13.13 Additional Liabilities

13.13.1 Liability for Cards Carrying the Marks

Each Principal is liable for Transactions that take place on its Cards and the Cards issued by any current or former Affiliate Sponsored by the Principal. The Principal's obligations hereunder are subject to the indemnity set forth in the Rules.

13.14 Issuer Assurance Plan

The Issuer Assurance Plan is supported within the Region.

Additional Regional Information

Latin America and the Caribbean Geographical Region

For further information refer to Appendix A, "Geographical Regions," in part 2 of this rulebook.

Technical Specifications

Refer to Appendix B, "Technical Specifications," in part 2 of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
1.7 Termination of License	A
4.1 Right to Use the Marks	A
4.2 Protection and Registration of the Marks	A
4.5 Display on Cards	B
5.3 A/CB Communication Standards	B
6.2 Card Standards and Specifications	A
6.10 Selective Authorization	B
7.1 Acquirer Obligations and Activities	A
7.4 Acquiring Electronic Commerce Transactions	A
7.17 Connection to the Interchange System	A
7.18 Card Capture	A
7.23 ATM Access Fees	B
9.2 POS Transaction Types	A
9.8 Authorizations	A
11.2 Exception Transaction Types	C

Chapter 19 South Asia/Middle East/Africa Region

This chapter contains Rule variances and additional Rules for the South Asia/Middle East/Africa Region.

Overview

Set forth below are the Rule variations to the Maestro Global Rules and additional Rules for the South Asia/Middle East/Africa Region. In most cases, the South Asia/Middle East/Africa chapter supplements part 1 of this rulebook and South Asia/Middle East/Africa Customers must comply with the Rules in both part 1 and Chapter 19, "South Asia/Middle East/Africa Region," of this rulebook.

If a subsection in the South Asia/Middle East/Africa regional chapter contains the full set of Rules applicable to South Asia/Middle East/Africa Customers, in place of the corresponding chapter in part 1 of this rulebook, then this is clearly mentioned, and South Asia/Middle East/Africa Customers are required to comply only with the Rules in that South Asia/Middle East/Africa chapter.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

Definitions

In addition to the defined terms in the "Definitions" chapter in part 1 of this rulebook, the following applies:

IVR Transaction

A non-face-to-face POS Transaction conducted by means of an interactive voice response (IVR) telephone system.

6.9 Electronic Commerce

In addition to the Rules in Chapter 6, "Issuing Requirements," Rule 6.9 in part 1 of this rulebook, with respect to intracountry electronic commerce Transactions that take place in India:

Issuers and their agents must support Payment Transactions and receive refunds for electronic commerce Transactions processed as Payment Transactions.

6.13 Issuer Responsibilities to Cardholders

In addition to the Rules in Chapter 6, "Issuing," Rule 6.13 in part 1 of this rulebook, the following apply:

1. Card Applications and Card Solicitations. Each Issuer shall disclose, clearly and conspicuously, in all Card applications and Card Solicitations any amounts in respect to the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
2. Existing Cardholder Agreements and Account Agreements. Each Issuer shall disclose, clearly and conspicuously, in all existing Cardholder agreements and Account agreements amounts in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
3. New Cardholder Agreements and Account Agreements. Each Issuer shall disclose, clearly and conspicuously, in all new Cardholder agreements and Account agreements amounts in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
4. Periodic Billing Statement. Each Issuer shall provide adequate disclosure on each applicable periodic billing statement, such that the Cardholder can readily determine from the billing statement any amounts that the Issuer charges to the Cardholder in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment during that billing cycle, either in gross or on a per Transaction basis.
5. Currency Conversion Procedure. The Corporation further recommends and encourages Customers to inform their Cardholders that part of the Corporation currency conversion procedure includes use of either a government-mandated exchange rate or a wholesale exchange rate, selected by the Corporation, and that the government-mandated exchange rate or wholesale exchange rate that the Corporation uses for a particular Transaction is the rate the Corporation selects for the applicable currency on the day the Transaction is processed, which may differ from that applicable to the date the Transaction occurred or when it is posted to the Cardholder's Account.

NOTE

Refer to the *Single Message System Specifications* for additional information about the MasterCard Currency Conversion Assessment. For information about the MasterCard Cross-border Assessment, refer to the *MasterCard Consolidated Billing System—SAMEA Region*.

7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only

7.2.4 Additional Acquiring Requirements

7.2.4.1 Interactive Voice Response (IVR) Transactions

Effective 1 January 2011, Merchants located in India may at their option offer IVR Transactions on Cards issued in India.

The Rules for IVR Transactions are the same as those for face-to-face POS Transactions except that:

1. IVR Transactions must not be performed using Maestro *PayPass* contactless payment functionality or include purchase with cashback Transactions;
2. manual key entry of the PAN is the normal method of performing an IVR Transaction;
3. the Merchant must support the passing of the data in UCAF to the Acquirer.
4. An Acquirer must provide each Merchant with a Merchant ID, and ensure that its Merchants correctly populate all UCAF fields with required data elements.
5. a zero floor limit is applicable for all IVR Transactions;
6. if an Issuer's response to an authorization request is incorrectly supplied as call referral, this must be translated into a decline;
7. the Merchant must not request an authorization until the goods or services are ready to be dispatched;
8. the Transaction receipt and the goods and/or services are not provided to the Cardholder upon completion of the Transaction, but rather are delivered to the Cardholder by a method chosen at the Merchant's discretion or collected by the Cardholder. Refer to the *MasterCard SecureCode—Merchant Implementation Guide* for more information.

7.4 Acquiring Electronic Commerce Transactions

7.4.1 Acquirer Responsibilities: Electronic Commerce Transactions

In addition to the Rules in Chapter 7, "Acquiring Requirements," Rule 7.4.1 in part 1 of this rulebook, with respect to intracountry electronic commerce Transactions that take place in India:

8. process refunds as Payment Transactions.

7.4.1.1 Merchant Requirements: Electronic Commerce Transactions

In addition to the Rules in Chapter 7, "Acquiring Requirements," Rule 7.4.1.1 in part 1 of this rulebook, with respect to intracountry electronic commerce Transactions that take place in India:

8. process refunds as Payment Transactions.

9.2 POS Transaction Types

9.2.2 Acquirer Online POS Transactions

9.2.2.2 Optional Online POS Transactions

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.2.2.2 in part 1 of this rulebook, the following applies:

3. Cash back without purchase

Merchants that have received approval from their Acquirer may offer cash back to a Cardholder without an accompanying purchase Transaction for intracountry Transactions conducted in India or South Africa.

9.4 Special Transaction Types

9.4.2 Processing Requirements—Electronic Commerce Unique Transaction Types and Payment Transactions

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.4.2 in part 1 of this rulebook, with respect to intracountry electronic commerce Transactions that take place in India:

Refunds for electronic commerce Transactions must be processed as Payment Transactions.

Additional Regional Information

South Asia/Middle East/Africa Geographical Region

For further information refer to Appendix A, "Geographical Regions," in part 2 of this rulebook.

Technical Specifications

Refer to Appendix B, "Technical Specifications," in part 2 of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this Maestro Global Rules manual.

Rule Number/Rule Title	Category
6.13 Issuer Responsibilities to Cardholders	B
7.2 Additional Acquirer Obligations and Activities for Acquiring Transactions from a Merchant—POS and Electronic Commerce Only	A

Chapter 20 United States Region

This chapter contains Rule variations and additional Rules for the United States Region.

Overview

Set forth below are the Rule variations to the *Maestro Global Rules* and additional Rules for the United States Region. In most cases, the United States Chapter supplements part 1 of this rulebook and United States Customers must comply with the Rules in both part 1 and Chapter 20, "United States Region," of this rulebook.

If a subsection in the United States regional Chapter contains the full set of Rules applicable to United States Customers, in place of the corresponding Chapter in part 1 of this rulebook, then this is clearly mentioned, and United States Customers are required to comply only with the Rules in that United States Chapter.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

The Maestro product is fully online, with a zero floor limit and real-time data capture. Cardholders interact with attended and unattended POS Terminals and Terminals that capture the data required for processing from the magnetic stripe or chip on the Card.

Definitions

In addition to the defined terms in the "Definitions" chapter in part 1 of this rulebook, the following applies:

Designee

An entity, including but not limited to, a Third Party Processor or a Merchant, that has been authorized by the Corporation to connect directly to the Interchange System.

3.7 Provision and Use of Information

3.7.5 Confidential Information of Third Parties

In addition to the Rules in Chapter 3, "Common Obligations," Rule 3.7.5 in part 1 of this rulebook, the following apply:

Solely for the purposes of this Rule 3.7.5:

1. "Work Product" will mean any report(s), specifications, documentation, or other deliverables (including any updates and modifications thereof) developed (in whole or in part) by Fair Isaac Corporation and provided to the Customer.
2. "Service" will mean the MasterCard Alert containing at-risk accounts from the Account Data Compromise (ADC) program.

3.7.5.1 Participation in the Service

Customers that participate in the Service through the Corporation must limit the use of the Work Product and the Service to:

1. any state of the United States of America, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States; and
2. the sole purposes of risk management or fraud detection by the Customer for the benefit of the Customer.

If a Customer uses the Work Product or the Service for any purpose other than those described above, including, but not limited to, use in connection with decisions regarding the approval or denial of credit or other products and services, that Customer's access to and right to utilize the Work Product and the Service will be terminated.

3.15 Integrity of Brand and Network

In addition to the Rules in Chapter 3, "Common Obligations," Rule 3.15 in part one of this rulebook, the following applies:

Pursuant to this Rule, with respect to any potentially illegal Internet gambling Transaction attempted on or after 1 June 2010, the Issuer of the Card must either employ a method of systemic Transaction blocking or decline all such Transaction authorization requests on an individual basis.

An Internet gambling Transaction that may be potentially illegal when involving a U.S. region Cardholder is any Transaction that the Acquirer has identified in the authorization request message as both

1. a gambling Transaction, by the use of MCC 7995 in DE 18 (Merchant Type), and
2. an e-commerce Transaction, by the use of a value of 6 (electronic commerce Transaction) in DE 61 (Point of Service [POS] Data), subfield 10 (Cardholder-Activated Terminal Level Indicator).

Issuers may approve, on an individual basis, any Internet gambling Transaction authorization requests identified with MCC 9754 (Gambling—Horse Racing, Dog Racing, State Lotteries) that involve a U.S. region Cardholder. In using MCC 9754, the Acquirer asserts that the Transaction involves gambling activity deemed by the Acquirer to be legal in the U.S. region. The Acquirer also acknowledges and agrees that the Transaction constitutes the Acquirer's Activity and is subject to Rule 13.14 of this rulebook, regardless of the Acquirer's compliance with the Corporation's *Internet Gambling Policy* or these requirements.

4.2 Protection and Registration of the Marks

In addition to the Rules in Chapter 4, "Marks," Rule 4.2 the following applies:

No use of a Mark may be made on or in connection with any card, device or other application associated with a payment service that the Corporation deems to be competitive with any Activity except as set forth in this chapter.

4.5 Display on Cards

The following replaces the second paragraph of Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook:

The Marks may be placed on a card in combination with any other local/regional/international POS debit mark and/or local/international ATM mark. In the event that a card has an international POS debit mark on the card front, and the card has a Maestro payment application:

1. if any other POS debit mark appears on the card back, the Marks must be displayed on the card back; or
2. if no other POS debit mark appears on the card back, the Marks are not required to appear on the card back.

A card must not include any visible indication communicating that acceptance or use of the Mark or the Maestro payment application is limited, geographically or otherwise.

The fifth paragraph of Chapter 4, "Marks," Rule 4.5 in part 1 of this rulebook in which Customers are prohibited from placing any other Competing EFT POS Network debit marks on their participating Cards does not apply.

4.6 Display of the Marks at POI Terminals

In addition to the Rules in Chapter 4, "Marks," Rule 4.6 in part 1 of this rulebook, the following applies:

The Marks may appear in conjunction with other regional or national network EFT Marks on devices that qualify as POS Terminals and Terminals.

6.1 Eligibility

6.1.1 Eligible Cards

The Rules set forth in Chapter 6, "Issuing," Rule 6.1.1 in part 1 of this rulebook are modified as set forth below.

A credit MasterCard card may be enhanced with the Maestro payment application.

6.2 Card Standards and Specifications

6.2.1 Encoding Standards

6.2.1.8 Application Software and Personalization of Maestro on Access Devices and Mobile Payment Devices

Effective 18 October 2013, an Issuer must ensure that each newly issued or reissued *PayPass*-enabled Card, Access Device, and Mobile Payment Device is personalized with the appropriate device type value.

6.2.3 Chip Card Standards

The Rules in Chapter 6, "Issuing," Rule 6.2.3 in part 1 of this rulebook are modified to include the following:

No payment application resident on a Chip Card issued in the U.S. region may have a higher application priority than the Card's primary application.

6.2.3.3 Card Authentication

The Rules in Chapter 6, "Issuing," Rule 6.2.3.3 in part 1 of this rulebook are modified as follows:

Any Chip Card issued or re-issued in the United States region:

1. May be configured to always require a POS Terminal to obtain online authorization from the Issuer for a contact chip Transaction. Such Cards are not required to support offline CAM for chip Transactions.
2. If configured to support offline authorization must support DDA or both DDA and CDA as the offline CAM(s) for contact chip Transactions and must not support SDA.

Any Maestro *PayPass* Card issued or re-issued in the United States region:

1. Must be configured to support both online and offline authorization of Maestro *PayPass* Transactions; and
2. Must support CDA as the offline CAM for Maestro *PayPass* Transactions and must not support SDA.

6.4 PIN and Signature Requirements

6.4.1 PIN Issuance

The following replaces the second paragraph of Chapter 6, "Issuing," Rule 6.4.1 in part 1 of this rulebook:

PINS must meet ISO standards, and may be from four (4) to twelve (12) alphanumeric characters.

6.4.2 Use of the PIN

6.4.2.1 Chip Cards

The Rules in Chapter 6, "Issuing," Rule 6.4.2.1 in part 1 of this rulebook are modified as follows:

1. Chip Cards may support either online PIN verification only or both online PIN and offline PIN verification as the CVM for POS Transactions.

6.4.3 Use of PIN or Signature

In addition to the rules in Chapter 6, "Issuing," Rule 6.4.3 in part 1 of this rulebook, the following applies:

For all intraregional Transactions the Cardholder utilizes a PIN for identification instead of a signature, except as provided for in the Rules.

6.7 Stand-In Processing Service

The following replaces Chapter 6, "Issuing," Rule 6.7 paragraph 2, in part 1 of this rulebook:

Issuers must support and implement Stand-In Processing for all POS Transactions.

In addition to the rules in Chapter 6, "Issuing," Rule 6.7 in part 1 of this rulebook, the following apply:

Stand-In Processing, a service that is supported by the Single Message System, is available to all Issuers twenty-four (24) hours a day, three hundred and sixty-five (365) days a year.

6.10 Selective Authorization

In addition to the Rules in Chapter 6, "Issuing," Rule 6.10 in part 1 of this rulebook, the following applies:

An Issuer may geographically restrict Card usage to the United States Region for a Card Program, except in the case of a prepaid Card Program, subject to the following requirements:

3. The Issuer must inform the Cardholder clearly in writing of the geographic scope of the Card;

4. The Issuer must also inform the Cardholder clearly in writing that he/she has the option of enabling expanded geographic use of the Card upon the Cardholder's request. An Issuer must comply with requests from Cardholders for expanded geographic use of a Card. If the Issuer cannot expand a Card's use to a specific country or a select group of countries as requested by the Cardholder, the Issuer must enable the Card for global use and must inform the Cardholder accordingly; and

5. The geographic restriction must be clearly printed on the Card back, for example, "For use only in the United States. To enable for use outside the United States, please call (Issuer)."

For additional information, refer to the *Card Design Standards* manual.

For purposes of this section, if an Issuer chooses to geographically restrict Card usage to the United States, the Issuer must permit Card usage in the U.S. Region, Puerto Rico, U.S. Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands.

6.13 Issuer Responsibilities to Cardholders

In addition to the Rules in Chapter 6, "Issuing," Rule 6.13 in part 1 of this rulebook, the following apply:

1. **Card Applications and Card Solicitations**. Each Issuer shall disclose, clearly and conspicuously, in all Card applications and Card Solicitations any amounts in respect to the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
2. **Existing Cardholder Agreements and Account Agreements**. Each Issuer shall disclose, clearly and conspicuously, in all existing Cardholder agreements and Account agreements amounts in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
3. **New Cardholder Agreements and Account Agreements**. Each Issuer shall disclose, clearly and conspicuously, in all new Cardholder agreements and Account agreements amounts in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment that the Issuer charges, or will charge, to the Cardholder.
4. **Periodic Billing Statement**. Each Issuer shall provide adequate disclosure on each applicable periodic billing statement, such that the Cardholder can readily determine from the billing statement any amounts that the Issuer charges to the Cardholder in respect of the MasterCard Issuer Cross-border Assessment and the MasterCard Currency Conversion Assessment during that billing cycle, either in gross or on a per Transaction basis.
5. **Currency Conversion Procedure**. The Corporation further recommends and encourages Customers to inform their Cardholders that part of the Corporation currency conversion procedure includes use of either a government-mandated exchange rate or a wholesale exchange rate, selected by the Corporation, and that the government-mandated exchange rate or wholesale exchange rate that the Corporation uses for a particular Transaction is the rate the Corporation selects for the applicable currency on the day the Transaction is processed, which may differ from that applicable to the date the Transaction occurred or when it is posted to the Cardholder's Account.

NOTE

Refer to the *Single Message System Specifications* for additional information about the MasterCard Currency Conversion Assessment. For information about the MasterCard Cross-border Assessment, refer to the *MasterCard Consolidated Billing System—United States Region*.

6.17 Additional Rules for Issuing

An Issuer must post funds due to a Cardholder as a result of a refund Transaction to the Cardholder's Account within one business day of Transaction settlement. The Issuer may place a temporary hold on such funds to the extent allowed under applicable law if the Issuer determines that the circumstances or Account history warrant the delay.

6.18 Shared Deposits

In addition to the Rules in Chapter 6, "Issuing," in part 1 of this rulebook, the following applies:

6.18.1 Participation Requirements

If an Issuer elects to take part in the Shared Deposit service, then that Issuer must designate its BINs and Terminals that participate in any other shared deposit service for participation in the Shared Deposit service.

6.18.2 Shared Deposits in Excess of USD 10,000

The Issuer is responsible for complying with the applicable requirements of the U.S. Bank Secrecy Act, and regulations promulgated thereunder, with respect to its Cardholder's Shared Deposit or series of related Shared Deposits made to a single Account on one (1) business day containing currency in excess of USD 10,000.

7.1 Acquirer Obligations and Activities

7.1.16 Acquirer Host System Requirements

Effective 19 April 2013, each United States region Acquirer must ensure that its POS Terminal host systems and those of its Service Providers:

1. Are capable of processing contact chip Transactions and Maestro *PayPass* Transactions,
2. Support the transmission of contact chip Transaction and Maestro *PayPass* Transaction messages in accordance with the Standards;
3. Support all mandatory and applicable conditional data subelements within DE 55 (Integrated Circuit Card [ICC] System-Related Data); and
4. Have been approved by the Corporation, with respect to each Interchange System network interface, as enabled for chip Transaction and Maestro *PayPass* Transaction processing.

7.4 Acquiring Electronic Commerce Transactions

7.4.1 Acquirer Responsibilities: Electronic Commerce Transactions

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.4.1 in part 1 of this rulebook, the following apply:

MCC 9754

A U.S. region Acquirer may register a Merchant to use MCC 9754 (Gambling—Horse Racing, Dog Racing) if the Merchant is located in the U.S. region and is engaged in gambling activity involving horse racing or dog racing. To register such a Merchant, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items to the Corporation as part of the registration process:

1. **Evidence of legal authority**. The Acquirer must provide:
   a. A copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority, that expressly authorizes the Merchant to engage in the gambling activity; and
   b. Any law applicable to the Merchant that permits the gambling activity.
2. **Legal opinion**. The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a private sector U.S. lawyer or U.S. law firm. The legal opinion must:
   a. Identify all relevant gambling, gaming, and similar laws applicable to the Merchant;
   b. Identify all relevant gambling, gaming, and similar laws applicable to Cardholders permitted by the Merchant to transact with the Merchant; and
   c. Demonstrate that the Merchant's and Cardholders' gambling and payment activities comply at all times with any laws identified above. The Acquirer must provide the Corporation with a copy of such legal opinion. The legal opinion must be acceptable to the Corporation in its sole discretion.
3. **Effective controls**. The Acquirer must provide certification from a qualified independent third party demonstrating that the Merchant's systems for operating its gambling business:
   a. Include effective age and location verification; and
   b. Are reasonably designed to ensure that the Merchant's Internet gambling business will remain within legal limits (including in connection with interstate transactions).

The certification must include all screenshots relevant to the certification (for example, age verification process). Certifications from interested parties (such as, the Acquirer, ISOs, the Merchant, and so on) are not acceptable substitutes for the independent third-party certification.

4. **Notification of changes**. The Acquirer must certify that it will notify MasterCard of any changes to the information it has provided to the Corporation, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to the Corporation (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten days of any such change.
5. **Acceptance of responsibilities**. The Acquirer must specifically affirm that it will not submit restricted transactions from the Merchant for authorization. The Acquirer must also specifically reaffirm its indemnification to the Corporation in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 13.14 of this rulebook regardless of the Acquirer's compliance with the Corporation's *Internet Gambling Policy* or these requirements.

MCC 9399

A U.S. region Acquirer may use MCC 9399 (Government Services—Not elsewhere classified) to identify Transactions arising from a U.S. region Merchant and involving the purchase of a state lottery ticket if the Acquirer has first registered the Merchant with the Corporation. To register such a Merchant, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items to the Corporation as part of the registration process:

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

opinion. The legal opinion must be acceptable to the Corporation in its sole discretion.

3. **Effective controls**. The Acquirer must provide certification from a qualified independent third party demonstrating that the Merchant's systems for operating its state lottery business.

   a. Include effective age and location verification; and

   b. Are reasonably designed to ensure that the Merchant's state lottery business will remain within legal limits (including in connection with interstate transactions).

   The certification must include all screenshots relevant to the certification (for example, age verification process). Certifications from interested parties (such as, the Acquirer, ISOs, the Merchant, and so on) are not acceptable substitutes for the independent third-party certification.

4. **Notification of changes**. The Acquirer must certify that it will notify MasterCard of any changes to the information it has provided to the Corporation, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to the Corporation (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten days of any such change.

5. **Acceptance of responsibilities**. The Acquirer must specifically affirm that it will not submit restricted transactions from the Merchant for authorization. The Acquirer must also specifically reaffirm its indemnification to the Corporation in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 13.14 of this rulebook regardless of the Acquirer's compliance with the Corporation's *Internet Gambling Policy* or these requirements.

MCC 7994

A U.S. region Acquirer may use MCC 7994 (Video Game Arcades/Establishements) to identify Transactions arising from a U.S. region Merchant conducting games (herein, "skill games") if the Acquirer has first registered the Merchant with the Corporation. The Acquirer may submit the registration request to the Corporation by sending an e-mail to internet_gambling@mastercard.com. For purposes of this section, "skill games" means:

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

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

1. **Evidence of legal authority**. The Acquirer must provide:

   a. A copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority, that expressly authorizes the Merchant to conduct the particular type of skill game(s) for which it wishes to accept Cards as payment for entry fees; and

   b. Any law applicable to the Merchant that permits the conduct of skill games.

2. **Legal opinion**. The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a private sector U.S. lawyer or U.S. law firm. The legal opinion must:

   a. Identify all relevant laws that address the conduct of skill games (*e.g.*, anti-gambling laws that provide an exemption for skill games) and other laws applicable to the Merchant's skill games activities;

   b. Identify all relevant laws that address the participation in skill games and other laws applicable to Cardholders permitted by the Merchant to participate in skill games with the Merchant; and

   c. Demonstrate that the Merchant's and Cardholders' skill games and payment activities comply at all times with any laws identified above.

   The Acquirer must provide the Corporation with a copy of such legal opinion. The legal opinion must be acceptable to the Corporation in its sole discretion.

3. **Effective controls**. The Acquirer must provide certification from a qualified independent third party demonstrating that the Merchant's systems for operating its skill games business:

   a. Include effective age and location verification; and

   b. Are reasonably designed to ensure that the Merchant's skill games business will remain within legal limits (including in connection with interstate Transactions).

   The certification must include all screenshots relevant to the certification (for example, age verification process). Certifications from interested parties (such as, the Acquirer, ISOs, the Merchant, and so on) are not acceptable substitutes for the independent third-party certification.

4. **Notification of changes**. The Acquirer must certify that it will notify MasterCard of any changes to the information it has provided to the Corporation, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to the Corporation (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.

5. **Acceptance of responsibilities**. The Acquirer must specifically affirm that it will not submit Restricted Transactions (as defined in the Internet Gambling Policy) from the Merchant for authorization. The Acquirer must also specifically reaffirm its indemnification to the Corporation in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 13.14 of this rulebook regardless of the Acquirer's compliance with the Corporation's *Internet Gambling Policy* or these requirements.

7.4.1.1 Merchant Requirements: Electronic Commerce Transactions

The following replaces the Rule in Chapter 7, "Acquiring," Rule 7.4.1.1 (1) in part 1 of this rulebook:

1. support MasterCard *SecureCode* or any alternative CVM that is supported on the MasterCard Worldwide Network so long as it has been approved by the Corporation.

7.9 POS Terminal and Terminal Requirements

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.9 in part 1 of this rulebook, the following applies:

Effective 19 April 2013, the *PayPass* reader of a POS Terminal located in the United States region must support *PayPass* version 3.0 or later.

7.9.2 Manual Key-Entry of PAN

The following replaces Chapter 7, "Acquiring," Rule 7.9.2 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.

7.9.3 PIN Entry Device

The following replaces Rule 7.9.3 (1) of Chapter 7, "Acquiring," in part 1 of this rulebook:

1. have an alphanumeric keyboard to enable the entry of PINs.

The following replaces Rule 7.9.3 (3) of Chapter 7, "Acquiring," in part 1 of this rulebook:

3. be capable of allowing entry of PINs having from four (4) to twelve (12) characters.

7.9.6 Balance Inquiry

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.9.6 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.

7.10 Hybrid POS Terminal and Hybrid Terminal Requirements

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.10 in part 1 of this rulebook, the following applies:

Effective 1 October 2015, the liability for intraregional counterfeit fraudulent Transactions in which one Customer (either the Issuer or the Acquirer) is not yet EMV chip-compliant is borne by the non–EMV chip-compliant Customer. This liability shift is effective 1 October 2017 for automated fuel dispenser Transactions (MCC 5542). For purposes of these Rules, "EMV chip-compliant" means in compliance with the Standards set forth in the *M/Chip Requirements* manual and other M/Chip documentation and with the EMV specifications then in effect.

7.11 Additional Requirements for POS Terminals

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.11 in part 1 of this rulebook, the following applies:

3. POS Terminals must contain keyboards that assign letter-number combinations as described in Rule 7.10 in part 1 of this rulebook.

4. Effective 19 April 2013, POS Terminals that utilize Maestro *PayPass* contactless functionality must transmit the device type indicator in DE 48, subelement 23 (Payment Initiation Channel), subfield 1 (Device Type) of authorization messages when such indicator is present in the Card, Access Device, or Mobile Payment Device used to effect a Transaction.

7.12 Additional Requirements for ATMs

The following replaces Chapter 7, "Acquiring," Rule 7.12 (2) in part 1 of this rulebook:

2. assign letter-number combinations as described in Rule 7.12 in part 1 of this rulebook

7.14 POI Terminal Transaction Log

The Rules in Chapter 7, "Acquiring," Rule 7.14 in part 1 of this rulebook apply, except that the inclusion of the Transaction code description on the Transaction log is optional.

7.17 Connection to the Interchange System

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.17 in part 1 of this rulebook, the following applies:

Connection to the Interchange System is limited to Principals or their Designees.

7.17.3 Certification and Testing

In addition to the Rules in Chapter 7, "Acquiring," Rules 7.17.3 and 7.17.8 in part 1 of this rulebook, the following apply:

Principals and their Designees directly connected to the Interchange System must test and certify with the Interchange System to ensure that such Principals and Designees and all Customers and Merchants indirectly connected to the Interchange System through such Principals or Designees comply with the requirements set forth in the Rules.

Each direct-connect Principal and its Designees must provide all required information to the Corporation for the purpose of establishing and testing the interface, to ensure that the Principal or its Designees are able to communicate with the Interchange System using the agreed-upon operational characteristics as defined in the technical specifications of the Corporation, and must undertake all the necessary activities to become certified.

A certification test script must be successfully executed by each direct-connect Principal and its Designees to gain access to the Interchange System.

Each time a direct-connect Principal, or its Designees make material changes to the software that interfaces to the Interchange System, a recertification test is required. The recertification test ensures that changes made by such a Principal or its Designees do not adversely impact another Customer or the Interchange System.

7.17.5 Telecommunications

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.17.5 in part 1 of this rulebook, the following applies:

Direct-connect Principals and their Designees must establish a telecommunications circuit equipped with a backup service, between their processing site and the Interchange System.

7.17.6 Interface

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.17.6 in part 1 of this rulebook, the following applies:

Direct-connect Principals and their Designees must maintain the necessary computer hardware and software to maintain the interface to the Interchange System in accordance with the Rules and the technical specifications of the Corporation.

7.17.7 Message Formats

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.17.7 in part 1 of this rulebook, the following applies:

All direct-connect Principals and their Designees must comply with the technical specifications set forth in the *Single Message System Specifications* manual.

7.17.11 Hours of Operation

The following replaces the Rules in Chapter 7, "Acquiring," Rule 7.17.11 in part 1 of this rulebook:

Direct-connect Principals and their Designees must notify the Corporation of their scheduled outages. Customers' hours of operation must be so defined as to meet the criteria of Chapter 9, "Processing Requirements," Rule 9.8 in part 1 of this rulebook.

7.17.11.1 Maintenance Events

Customers must provide the Corporation with written notification of downtime required for maintenance events at least forty-eight (48) hours before any regularly scheduled maintenance events.

For emergency maintenance, Customers must provide the Corporation with written notification within five (5) business days after the occurrence of such event.

7.17.11.2 Written Notification

Written notification must include:

1. the date of the maintenance;
2. the times at which the maintenance commences and concludes; and
3. a brief description of the reason for the maintenance.

Written notification regarding emergency maintenance must also include a description of the actions taken to prevent a reoccurrence of the event.

	Scheduled Maintenance	Emergency Maintenance
Permissible Maintenance Time Frame	01:00 to 05:00(New York time)	Anytime
Maximum Hours per Month	10	4
Maximum Hours per Week	5	2
Maximum Hours per Day	2	1
Maximum Duration of Event (Hours)	2	1

7.18 Card Capture

7.18.1 POS Transactions

In addition to the Rules in Chapter 7, "Acquiring," Rule 7.18.1 in part 1 of this rulebook, the following applies:

The capture of Cards at POS Terminals is prohibited.

7.23 ATM Access Fees

7.23.1 Domestic Transactions

The following replace Chapter 7, "Acquiring," Rule 7.23.1, paragraph 1 in part 1 of this rulebook:

In all states and territories of the United States and in the District of Columbia, upon complying with the ATM Access Fee certification requirements of the Rules, United States Acquirers may assess an ATM Access Fee on a Transaction at a Terminal if the Transaction is initiated with a Card issued in the United States.

Rules governing the imposition of ATM Access Fees must be followed and are contained in this Chapter 20, Rule 7.23.1 of this rulebook.

7.23.1.1 Transaction Field Specifications

At the time of each disbursement Transaction on which an ATM Access Fee is imposed, the Acquirer of such Transaction must transmit, in the field specified by the *Single Message System Specifications* manual, the amount of the ATM Access Fee separately from the amount of the cash disbursed in connection with such Transaction.

7.23.1.2 Non-discrimination Regarding ATM Access Fees

An Acquirer must not charge an ATM Access Fee in connection with a Transaction that is greater than the amount of any ATM Access Fee charged by that Acquirer in connection with the transactions of any network accepted at that Terminal.

7.23.1.3 Notification of ATM Access Fee

An Acquirer that plans to add an ATM Access Fee must notify its Sponsoring Principal, in writing, of its intent to do so prior to the planned first imposition of such ATM Access Fee by the Acquirer.

The Principal must update the Location Administration Tool (LAT) regarding its or its Affiliates' imposition of ATM Access Fees.

7.23.1.4 Cancellation of Transaction

Any Acquirer that plans to add an ATM Access Fee must notify the Cardholder with a screen display that states the ATM Access Fee policy and provides the Cardholder with an option to cancel the requested Transaction.

7.23.1.5 Terminal Signage, Screen Display, and Transaction Record Requirements

Any Acquirer that plans to add an ATM Access Fee to a Transaction must submit a proposed Terminal, screen display, and receipt "copy" that meets the requirements of the Rules to it Sponsoring Principal in writing for approval prior to use, unless such Acquirer employs the model form (see Appendix D, "Signage, Screen, and Receipt Text Displays" in part 2 of this rulebook).

The Sponsoring Principal has the right to determine the acceptability of any new or changes to previously approved signage, screen display, and receipt copy. In cases of conflict between the Acquirer and its Sponsoring Principal, the Corporation has the sole right to determine the acceptability of any and all signage, screen display, and receipt copy.

7.23.1.5.1 Additional Requirements for Terminal Signage

An Acquirer that plans to add an ATM Access Fee to a Transaction may optionally display signage that is clearly visible to Cardholders on or near all Terminals at which ATM Access Fees apply.

The minimum requirement for ATM Access Fee signage text is wording that clearly states:

1. the name of the ATM Owner and Principal;
2. that the Transaction will be subject to an ATM Access Fee that will be deducted from the Cardholder's Account in addition to any Issuer fees;
3. the amount of, calculation method of, or Corporation-approved generic signage regarding the ATM Access Fee;
4. that the ATM Access Fee is assessed by the Acquirer instead of the Issuer;
5. that the ATM Access Fee is assessed on United States Cardholders only.

The minimum requirements for Terminal signage (physical characteristics) are as follows:

1. the signage must bear the heading "Fee Notice";
2. the size of the Terminal signage must be a minimum of four (4) inches in height by four (4) inches in width;
3. the text must be clearly visible to all. It is recommended that the text be a minimum of fourteen (14) point type;
4. the heading must be clearly visible to all. It is recommended that the text be a minimum of eighteen (18) point type.

A model for Terminal signage regarding ATM Access Fee application, and an approved Spanish-language version is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook. If the Spanish-language version is used, the English-language version also must be displayed.

7.23.1.5.2 Additional Requirements for Terminal Screen Display

An Acquirer that plans to add an ATM Access Fee to a Transaction must present a screen display message that is clearly visible to Cardholders on all Terminals at which ATM Access Fees apply. If the Cardholder is given the option of choosing a preferred language in which to conduct the Transaction, the screen display message concerning ATM Access Fees must be presented to the Cardholder in that chosen language.

If an Acquirer displays the Corporation-approved generic ATM Access Fee signage, the Acquirer must include the amount or calculation method of the ATM Access Fee as part of the Terminal screen display.

A model for the Terminal screen display regarding ATM Access Fee application, and an approved Spanish language version is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook. If the Spanish-language version is used, the English-language version must also be displayed.

7.23.1.5.3 Additional Requirements for Transaction Records

Any Acquirer that adds an ATM Access Fee to a Transaction must make available to the Cardholder on its Terminal receipt the ATM Access Fee information required by this Rule 7.23.1.5.3, in addition to any other information the Acquirer elects to or is required to provide.

The minimum requirements for the Terminal receipt are:

1. a statement of the amount disbursed to the Cardholder;
2. a statement of the ATM Access Fee amount with language clearly indicating it is a fee imposed by the Acquirer;
3. a separate statement of the combined amount of the ATM Access Fee and the disbursed amount, with language clearly indicating that this amount will be deducted from the Cardholder's Account.

A model for the Terminal receipt text regarding ATM Access Fee application is contained in Appendix D, "Signage, Screen, and Receipt Text Displays," in part 2 of this rulebook.

7.25 Shared Deposits

In addition to the Rules in Chapter 7, "Acquiring," in part 1 of this rulebook, the following applies:

7.25.1 Participation Requirements

An Acquirer may optionally choose to participate in the Shared Deposit service. However, if an Acquirer deploys ATMs that participate in any other shared deposit service, those ATMs must participate in the Shared Deposit service.

An Acquirer may make only its Terminals available for participation in the Shared Deposit service. However, an Acquirer that as an Issuer elects to take part in the Shared Deposit service must designate its BINs and Terminals that participate in any other shared deposit service for participation in the Shared Deposit service.

7.25.2 Non-discrimination

Acquirers may impose a dollar limit on Shared Deposits accepted at a Terminal provided that the limit imposed on Cardholders is the same or more favorable than the limits imposed on cardholders of other networks. Thisdoes not limit the application of other Non-discrimination provisions contained in the Rules.

7.25.3 Terminal Signs and Notices

Acquirers must display a notice regarding funds availability in accordance with section 229.18(c) of Regulation CC, 12 C.F.R. § 229.18(c) on each Terminal that participates in the Shared Deposit service.

7.25.4 Maximum Shared Deposit Amount

The maximum Shared Deposit Transaction amount must be limited to USD 99,999.99.

7.25.5 Terminal Clearing

An Acquirer that accepts Shared Deposits must clear its Terminals at least once each business day.

7.25.6 Deposit Verification

An Acquirer must process its Shared Deposits as follows:

1. the Acquirer must complete an examination of each Shared Deposit no later than one (1) business day after the date of the Transaction;
2. such examination must be conducted under dual control standards by:
   a. two (2) employees of the Acquirer; or
   b. one (1) or more employees of the Acquirer with a surveillance camera monitoring the examination
3. the examination must consist of the following;
   a. the deposit must be verified to ensure that:
      - the dollar amount of the deposit keyed by the Cardholder at the Terminal matches the deposit contents
      - the deposit envelope is not empty; and
      - the deposit envelope does not contain only non-negotiable items
   b. the Acquirer must identify any irregularities that would make an item in the deposit envelope non-negotiable, such as:
      - the deposited currency is counterfeit;
      - the deposited currency, check or money order is in a denomination other than U.S. region currency;
      - the item is drawn on or payable by an institution located outside the U.S. region;
      - the item has a passbook attached;
      - the item is a photocopy;

- the item is a certificate of deposit or banker's acceptance;
- the item is a non-negotiable writing;
- the item is a returned or cancelled check or draft;
- a date is not present on the item;
- the item is postdated;
- the item is dated more than six (6) months prior to the date of the deposit;
- the payee field has not been completed;
- either the written or numeric amount does not appear on the item;
- the written amount does not match the numeric amount on the item;
- the amount on the item appears altered;
- the item includes restrictive wording;
- the item is missing an endorsement;
- the item, which requires a signature, is unsigned

4. the Acquirer must submit an adjustment within one (1) business day of the deposit verification date if a discrepancy exists between the deposit amount and the amount keyed into the Terminal. For additional information, refer to this Chapter 20, Rule 11.3.5.

7.25.7 Deposit Processing

By the end of the business day following the day on which a Terminal was cleared pursuant to Rule 7.25.5, "Terminal Clearing" above, the Acquirer must forward for collection all Shared Deposits cleared from that Terminal in the same manner it would forward its own Cardholders' deposits except as permitted under Rule 11.3 of Chapter 20, "United States Region," of this rulebook.

7.25.8 Shared Deposits in Excess of USD 10,000

If an Acquirer receives a Shared Deposit or series of related Shared Deposits made to a single Account on one (1) business day containing currency in excess of USD 10,000, the Acquirer must notify the Issuer of this fact by telephone, facsimile, or any other means permitted by the Corporation within two (2) business days of the date of deposit. The Acquirer must record the occurrence as well as the act of reporting the occurrence and must include the name of the Issuer's employee that received notification.

The notification must include the following:

1. cardholder number;
2. amount of currency;
3. amount of currency in bills of denomination of USD 10,000 or higher;
4. Terminal location; and
5. date and time of deposit.

If the Acquirer fails to provide notification of such a cash deposit(s) and the Issuer is assessed penalties or fines as a result of the Acquirer's failure, the Acquirer must indemnify the Issuer for such penalties and fines. For additional information, refer to Chapter 12, "Arbitration and Compliance" in part 1 of the Rules.

7.25.9 Notice of Return

If an item sent by an Acquirer to the payor bank of the item for presentment is returned to the Acquirer for any reason or the Acquirer receives notice of nonpayment of the item for any reason from the payor bank, the Acquirer must notify the Issuer of the receipt of such return or notice, and must initiate return of the returned item to the Issuer no later than one (1) business day following the receipt of the returned item or the notice of nonpayment, whichever is received first. Such notice to the Issuer must include the reason for nonpayment as set forth on the returned item or notice of nonpayment received. For additional information, refer to Chapter 11, "Exception Item Processing," in part 1 of the Rules.

9.2 POS Transaction Types

9.2.1 Issuer Online POS Transactions

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.2.1 in part 1 of this rulebook, the following applies:

12. balance inquiry

Issuers must support the following Transaction types:

1. preauthorization from pooled Account
2. partial approval from primary Account
3. partial approval from checking Account
4. partial approval from savings Account
5. partial approval from pooled Account
6. full and partial reversal
7. balance response for prepaid Card Account

9.2.2 Acquirer Online POS Transactions

9.2.2.1 Required Transactions

The following replaces Chapter 9, "Processing Requirements," Rule 9.2.2.1 (2) 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.

In addition, the Acquirer of a Merchant included in an MCC listed below must ensure that by the effective date indicated for such MCC:

1. For all Card-present Transactions occurring at an attended POS Terminal or at a Cardholder-activated Terminal (CAT) identified with MCC 5542, the Merchant supports partial approvals.
2. For all Transactions, the Merchant supports full and partial reversals.
3. For all Card-present Transactions occurring at an attended POS Terminal and conducted with a prepaid Card, the Merchant supports account balance responses.

Effective Date	MCC	Description
1 May 2010	5310	Discount Stores
	5311	Department Stores
	5411	Grocery Stores, Supermarkets
	5499	Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores and Vending Machines
	5541	Service Stations (with or without Ancillary Services)
	5542	Fuel Dispenser, Automated
	5812	Eating Places, Restaurants

Effective Date	MCC	Description
	5814	Fast Food Restaurants
	5912	Drug Stores, Pharmacies
	5942	Book Stores
1 May 2010	5943	Office, School Supply and Stationery Stores
	7829	Motion Picture-Video Tape Production-Distribution
	7832	Motion Picture Theaters
	7841	Video Entertainment Rental Stores
	8011	Doctors—not elsewhere classified
	8021	Dentists, Orthodontists
	8099	Health Practitioners, Medical Services—not elsewhere classified
	5111	Stationery, Office Supplies
	5200	Home Supply Warehouse Stores
	5331	Variety Stores
	5399	Miscellaneous General Merchandise Stores
	5732	Electronic Sales
	5734	Computer Software Stores
	5735	Record Shops
	5921	Package Stores, Beer, Wine, and Liquor
	5941	Sporting Goods Stores
	5999	Miscellaneous and Specialty Retail Stores
	8041	Chiropractors
	8042	Optometrists, Ophthalmologists
	8043	Opticians, Optical Goods, and Eyeglasses
	4812	Telecommunication Equipment including Telephone Sales
	4814	Telecommunication Services
	5300	Wholesale Clubs
	5964	Direct Marketing—Catalog Merchants
	5965	Direct Marketing—Combination Catalog—Retail Merchants

Effective Date	MCC	Description
	5966	Direct Marketing—Outbound Telemarketing Merchants
	5967	Direct Marketing—Inbound Telemarketing Merchants
	5969	Direct Marketing—Other Direct Marketers—not elsewhere classified
1 May 2010	8062	Hospitals
1 November 2010	4111	Transportation—Suburban and Local Commuter Passenger, including Ferries
	4816	Computer Network/Information Services
	4899	Cable, Satellite, and Other Pay Television and Radio Services
	7996	Amusement Parks, Carnivals, Circuses, Fortune Tellers
	7997	Clubs—Country Membership
	7999	Recreation services—not elsewhere classified
1 May 2011	8999	Professional Services—not elsewhere classified
	9399	Government Services—not elsewhere classified

NOTE

For the purposes of this section, stand-alone terminals means terminals that are not integrated into a merchant's POS system, such that the transaction amount must be manually entered into the terminal.

Acquirers for merchants with card acceptor business codes (MCCs) listed in this table as effective 1 May 2010 or 1 November 2010 must support these requirements in all stand-alone terminal software updates performed after 1 May 2010 and for all stand-alone terminals that are deployed after 1 May 2010.

9.2.2.2 Optional Online POS Transactions

Partial approval, full and partial reversals, and account balance responses are required transactions for Acquirers and Merchants in certain Merchant Category Codes (MCCs), as specified in Rule 9.2.2.1.

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.2.2.2 (2.b) 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 Rule 9.2.2.2 (2.e) 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.

9.3 Terminal Transaction Types

9.3.1 Issuer Requirements

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.3.1 in part 1 of this rulebook, the following applies:

Issuers must offer to each Cardbase that offers access to an Account, as applicable, the following Transactions:

1. cash withdrawal from a savings Account
2. cash withdrawal from a checking Account

9.3.1.1 Issuer—Optional Transactions

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.3.1.1 in part 1 of this rulebook, the following applies:

1. Shared Deposit to savings Account
2. Shared Deposit to checking Account

9.3.2 Acquirer Requirements

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.3.2 in part 1 of this rulebook, the following applies:

Terminals must offer the following Transactions to the extent permitted by law or regulation or both:

1. cash withdrawal from a savings Account
2. cash withdrawal from a checking Account
3. cash advance from credit card
4. balance inquiry—checking Account
5. balance inquiry—savings Account
6. balance inquiry—credit card
7. transfer from checking to savings Account
8. transfer from savings to checking Account
9. Shared Deposit to savings Account if the Terminal accepts shared deposits for any other shared deposit service
10. Shared Deposit to checking Account if the Terminal accepts shared deposits for any other shared deposit service

All Terminals that perform cash withdrawals not requiring account selection must convert those Transactions to withdrawal from no Account specified.

9.3.2.1 Acquirer—Optional Transactions

The following replaces the first paragraph in Chapter 9, "Processing Requirements," Rule 9.3.2.1 in part 1 of this rulebook:

Terminals may offer a cash withdrawal from no Account specified to the extent permitted by law, regulations, or both.

Terminals may offer Shared Deposit to savings Account or checking Account if the Terminal does not accept shared deposits for any other shared deposit service.

9.8 Authorizations

9.8.2 Transaction Routing

In addition to the rules in Chapter 9, "Processing Requirements," Rule 9.8.2 in part 1 of this rulebook, the following apply:

Whenever a Card issued in the United States is used at an ATM in the United States Region for a Transaction other than the purchase of Merchandise and the Mark is a common brand, but not the only common brand, on the Card and the ATM, the resulting Transaction must be routed to the interchange system specified by the Issuer.

Whenever a Card issued in the United States Region is used at an ATM in the United States Region for a Transaction other than the purchase of Merchandise, the Transaction must be routed to the Interchange System unless the Issuer informs the Corporation that it has specified an interchange system other than the Interchange System.

9.8.7 Authorization Response Time

9.8.7.1 Issuer Response Time Requirements

In addition to the Rules in Chapter 9, "Processing Requirements," Rule 9.8.7.1 in part 1 of this rulebook, the following apply:

Principals 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 *Single Message System Specifications* manual.

9.8.7.2 Acquirer Response Time Requirements

The following replace Chapter 9, "Processing Requirements," paragraphs 1 and 2 of Rule 9.8.7.2 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.

9.9 Performance Standards

9.9.1 Issuer Standards

The following replaces Chapter 9, "Performance Standards," Rules 9.9.1.1 and 9.9.1.2 in part 1 of this rulebook.

9.9.1.1 Issuer Failure Rate

An Issuer failure rate that exceeds two percent (2%) for POS or ATM Transactions in any given month is considered substandard performance. The Issuer failure rate will not apply to a Processor until:

1. After the fourth calendar month of operation; or
2. Upon processing five thousand (5,000) Transactions in a calendar month; whichever occurs first.

Issuers that have been designated by the Corporation as having substandard performance may be subject to noncompliance assessments.

10.2 Settlement

In addition to the Rules in Chapter 10, "Settlement and Reconciliation," Rule 10.2 in part 1 of this rulebook, the following applies:

The Interchange System only provides Settlement/reconciliation services to Principals, Acquiring Customers and/or their processors.

Principals are responsible for Settlement with their Sponsored Customers, and Merchants.

10.2.3 Settlement Currency

All Transactions must be settled in U.S. currency; internationally acquired Transactions will be converted to U.S. currency at exchange rates determined by the Corporation.

10.3 Reconciliation

In addition to the Rules in Chapter 10, "Settlement and Reconciliation," Rule 10.3 in part 1 of this rulebook, the following applies:

Principals are responsible for reconciliation with their Sponsored Customers, and Merchants.

13.8 Pre-authorized Transactions

The following replaces Chapter 13, "Liabilities and Indemnification," paragraph 1 of Rule 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.

13.10 Manually-entered PAN

In addition to the Rules in Chapter 13 "Liabilities and Indemnification," in part 1 of this rulebook, the following applies:

An Issuer is not liable to the Acquirer for Transactions completed at a Merchant through manual entry of a PAN that is accepted by the Issuer and subsequently determined to have been generated through use of a fraudulent Card and/or unauthorized use of a PIN.

13.13 Additional Liabilities

In addition to the Rules in Chapter 13, "Liabilities and Indemnification," in part 1 of this rulebook, the following applies:

The Corporation reserves the right to adopt financial responsibility requirements for Customers. Such criteria may be instituted to comply with future laws or regulations, or for reasons of financial prudence on the part of the Corporation.

13.13.1 Liability for Shared Deposits

The maximum damages that an Acquirer may face for its failure to comply with these Shared Deposit Rules is the amount of loss incurred by the Issuer with respect to a particular Shared Deposit (such amount not to exceed the amount of the Shared Deposit).

In addition, an Acquirer will not be liable to an Issuer for any amount of the Shared Deposit that the Issuer could have recovered from the Cardholder. An Issuer must claim that:

1. its Cardholder would not accept the adjustment of an improper Shared Deposit;
2. it could not debit the Cardholder when the Issuer received notice of the improper deposit; and
3. it could have debited the Cardholder if the Acquirer had complied with these Shared Deposit rules.

In all events, the Issuer must first attempt to collect from its Cardholder.

Additional Regional Information

United States Geographical Region

For information refer to Appendix A, "Geographical Regions," in part 2 of this rulebook.

Technical Specifications

Refer to Appendix B, "Technical Specifications," in part 2 of this rulebook.

Screen and Receipt Text Displays

For information refer to Appendix D, "Screen and Receipt Text Displays," in part 2 of this rulebook.

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this Chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
3.15 Integrity of Brand and Network	A
4.2 Protection and Registration of the Marks	B
4.5 Display on Cards	B
4.6 Display of the Marks at POI Terminals	B
6.4 PIN and Signature Requirements	A
6.7 Stand-In Processing Service	A
6.13 Issuer Responsibilities to Cardholders	B
6.17 Additional Rules for Issuing	B
6.18 Shared Deposits	B
7.9 POS Terminal and Terminal Requirements	A
7.11 Additional Requirements for POS Terminals	A
7.12 Additional Requirements for ATMs	A
7.14 POI Terminal Transaction Log	A
7.17 Connection to the Interchange System	A
7.18 Card Capture	A
7.23 ATM Access Fees	B
7.25 Shared Deposits	B
9.2 POS Transaction Types	A
9.3 Terminal Transaction Types	A
9.8 Authorizations	A
9.9 Performance Standards	A
10.2 Settlement	A
10.3 Reconciliation	A

Chapter 21 Maestro PayPass

This chapter contains Rule variations or additional Rules applicable to Maestro PayPass.

Overview

Set forth below are the Rule variations to the *Maestro Global Rules* for Maestro® *PayPass*™ contactless payment functionality. In most cases, the Maestro *PayPass* chapter supplements part 1 of this rulebook and Customers must comply with the Rules in both part 1 and Chapter 21, "Maestro *PayPass*," of this rulebook.

If a subsection in the Maestro *PayPass* chapter contains the full set of Rules applicable to Maestro *PayPass*, this is clearly mentioned, and the Customers must comply with the Rules in Chapter 21, "Maestro *PayPass*," of this rulebook.

In all cases, Customers should refer to part 1 of this rulebook in the first instance.

Where approved by the Corporation (either on a country-by-country or case-by-case basis), Acquirers may Sponsor Merchants that deploy point-of-sale (POS) Terminals that utilize only the Maestro *PayPass* contactless payment functionality. Each Acquirer must ensure that, should any of its Merchant(s) approved by the Corporation to deploy POS Terminals that utilize only the Maestro *PayPass* contactless payment functionality subsequently deploy POS Terminals that comply with the requirements set forth in Rule 7.9 of this rulebook, such compliant POS Terminals accept and properly process Transactions.

The Corporation has approved the following:

- Merchants that deploy single-vehicle parking meters (MCC 7523)
- Merchants that deploy single-ride bus fare collection devices (MCC4131)
- Merchants that use the following MCCs:
  - MCC 4111—Transportation—Suburban and Local Commuter Passenger, including Ferries
  - MCC 4112—Passenger Railways
  - MCC 4789—Transportation Services—not elsewhere classified
- Merchants located in Belgium, Canada, Germany, Italy, Poland, Slovenia, the Netherlands, Spain, Switzerland, Turkey, Ukraine, or the United Kingdom that deploy any type of parking meters, including multiple-vehicle parking meters (MCC 7523).
- Merchants located in Germany, Poland, Slovenia, Spain, Switzerland, Turkey, Ukraine, or the United Kingdom that deploy "select first" vending machines (MCC 5499).
- Subject to Corporation approval on a case-by-case basis, Merchants at mass events, festivals, and sports arenas located in Hungary, Poland, and the United Kingdom that use the following (MCCs):
  - MCC 7941—Athletic Fields, Commercial Sports, Professional Sports Clubs, Sports Promoters
  - MCC 7929—Bands, Orchestras, and Miscellaneous Entertainers not elsewhere classified
  - MCC 5811—Caterers
  - MCC 7922—Theatrical Producers (except Motion Pictures), Ticket Agencies
  - MCC 7999—Recreational Services—not elsewhere classified
- Merchants located in Poland that use MCC 5994—News Dealers and Newsstands.

Refer to Rule 9.13 for information regarding the ceiling limit values that apply to Maestro *PayPass* Transactions.

2.2 License Application

2.2.2 *PayPass* License

All Customers must have been granted the appropriate *PayPass* licenses before using *PayPass* technology.

7.1 Acquirer Obligations and Activities

7.1.8 Card Acceptance Requirements for Maestro *PayPass*-only Merchants

The following Rules replace the corresponding subsections of Chapter 7, "Acquiring," Rule 7.1.8 in part 1 of this rulebook:

Each Acquirer must ensure that a Merchant, which has been approved by the Corporation to deploy POS Terminals that utilize only the Maestro *PayPass* contactless payment functionality:

1. does not require, or post signs indicating that it requires a minimum Transaction amount to accept a valid Card;
2. understands that it does not need to deploy a POS Terminal that contains a PIN entry device as CVM is not required;
3. complies with the Standards and all applicable laws and regulations, including but not limited to the "PAN Truncation Requirements" set forth in Chapter 7, "Acquiring," of part 1 of this rulebook, if the Merchant provides the Cardholder with a receipt.

NOTE

Regional Rule variations on this topic appear in Chapter 17, "Europe Region," of this rulebook.

7.9 POS Terminal Requirements

The following Rules replace Chapter 7, "Acquiring," Rule 7.9 and Rule 7.10, in part 1 of this rulebook:

All eligible POS Terminals that utilize only Maestro *PayPass* contactless payment functionality must:

1. perform Transactions only after receiving authorization from the Issuer or the Chip Card;
2. provide operating instructions in English as well as the local language;
3. have a screen display that enables the Cardholder to view the data entered into the POS 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;
4. prevent additional Transactions from being entered into the system while a Transaction is being processed;
5. perform the Transaction using the EMV chip;
6. read and process all required Maestro *PayPass*-related data from the EMV chip on the Card;
7. comply with the acceptance requirements set forth in the Maestro *PayPass* technical specifications, as published from time to time by the Corporation;
8. meet the *PayPass* M/Chip certification requirements, excluding the *PayPass* magnetic stripe profile;
9. have completed the Corporation's prescribed certification process for the appropriate environment of use, including the certification of the Acquirer's host interface;
10. request a cryptogram for all Maestro *PayPass* Transactions; if the Transaction is approved, transmit an application cryptogram and related data; and
11. support both online and offline authorization.

7.9.1 Card Reader

POS Terminals that utilize only the Maestro *PayPass* contactless payment functionality are not required to contain a magnetic stripe reader.

7.9.2 Manual Key-Entry of PAN

Transactions must not be performed if the chip on the Card cannot be read for any reason.

7.9.3 PIN Entry Device

POS Terminals that utilize only the Maestro *PayPass* contactless payment functionality are not required to contain a PIN entry device.

7.15 Requirements for Transaction Receipts

The following rule replaces Chapter 7, "Acquiring," Rule 7.15 in part 1 of this rulebook:

POS Terminals that utilize only the Maestro *PayPass* contactless payment functionality at Merchants using the following MCCs are not required to provide a Transaction receipt at the time the Transaction is conducted; however, the Merchant must have a means by which to provide a receipt to the Cardholder upon request. If such means involves the storage, transmission, or processing of Account data, then it must comply with the Payment Card Industry Data Security Standard (PCI DSS). The manner in which to request a receipt must be clearly displayed at the Merchant location and in compliance with the requirements set forth in Rules 7.15.1, 7.15.5, 7.15.6, 7.15.7, and 7.15.8 in part 1 of this rulebook.

- MCC 4111—Transportation—Suburban and Local Commuter, Passenger, including Ferries
- MCC 4112—Passenger Railways
- MCC 4131—Bus Lines
- MCC 4789—Transportation Services—not elsewhere classified
- MCC 7523—Automobile Parking Lots and Garages

Compliance Zones

The following table provides the noncompliance category that the Corporation has assigned to the Standards described within this Chapter. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework, as described in Chapter 3 of this *Maestro Global Rules* manual.

Rule Number/Rule Title	Category
2.2 License Application	A
7.1 Acquirer Obligations and Activities	A
7.9 POS Terminal Requirements	A

Appendix A Geographical Regions

A.1 Asia/Pacific Region

The Asia/Pacific Region includes the following countries or territories.

- American Samoa
- Australia
- Brunei Darussalam
- Cambodia
- China
- Christmas Island
- Cocos (Keeling) Islands
- Cook Islands
- Fiji
- French Polynesia
- Guam
- Heard and McDonald Islands
- Hong Kong
- Indonesia
- Japan
- Kiribati
- Korea, Republic of
- Lao People's Democratic Republic
- Macao
- Malaysia
- Marshall Islands
- Micronesia, Federated States of
- Mongolia
- Nauru
- New Caledonia
- New Zealand
- Niue
- Norfolk Island
- Northern Mariana Islands
- Palau
- Papua New Guinea

- Philippines
- Pitcairn
- Samoa
- Singapore
- Solomon Islands
- Taiwan
- Thailand
- Timor-Leste
- Tokelau
- Tonga
- Tuvalu
- U.S. Minor Outlying Islands
- Vanuatu
- Viet Nam
- Wallis and Futuna

A.2 Canada Region

The Canada Region is composed of Canada.

A.3 Europe Region

The Europe Region includes the following countries or territories.

- Albania
- Andorra
- Antarctica
- Armenia
- Austria
- Azerbaijan
- Belarus
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Channel Islands (Guernsey, Jersey)
- Croatia

- Cyprus
- Czech Republic
- Denmark (Faroe Islands)
- Estonia
- Faroe Islands
- Finland (Aland Islands)
- France[1]
- Georgia
- Germany, Republic of
- Gibraltar
- Greece
- Greenland
- Hungary
- Iceland
- Ireland
- Isle of Man
- Israel
- Italy
- Kazakhstan
- Kosovo
- Kyrgyzstan
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Macedonia
- Malta
- Moldova, Republic of
- Monaco
- Montenegro, Republic of
- Netherlands
- Norway (Svalbard, Jan Mayen)

1. Includes Mayotte, Guadeloupe, Martinique, French Guiana, St. Martin, and St. Barthélemy.

- Poland
- Portugal
- Romania
- Russian Federation
- San Marino
- Serbia
- Slovakia
- Slovenia
- Spain
- St. Helena, Ascension and Tristan Da Cunha
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Tajikistan
- Turkey
- Turkmenistan
- Ukraine
- United Kingdom (Falkland Islands, Malvinas)
- Uzbekistan
- Vatican City

Changes in allegiance or national affiliation of a part of any of the countries listed in this appendix shall not affect the geographic coverage of the definition.

A.3.1 Single European Payments Area (SEPA)

The Single European Payments Area includes the following countries or territories.

- Andorra
- Austria
- Belgium
- Bulgaria
- Channel Islands
- Cyprus
- Czech Republic
- Denmark

- Estonia
- Finland
- France
- Germany
- Gibraltar
- Greece
- Hungary
- Iceland
- Ireland
- Isle of Man
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Monaco
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- San Marino
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom
- Vatican City

A.4 Latin America and the Caribbean Region

The Latin America and the Caribbean Region includes the following countries or territories.

- Anguilla
- Antigua and Barbuda
- Argentina
- Aruba
- Bahamas
- Barbados
- Belize
- Bermuda
- BES Islands[2]
- Bolivia
- Brazil
- Cayman Islands
- Chile
- Colombia
- Costa Rica
- Curacao
- Dominica
- Dominican Republic
- Ecuador
- El Salvador
- Grenada
- Guatemala
- Guyana
- Haiti
- Honduras
- Jamaica
- Mexico
- Montserrat
- Nicaragua
- Panama
- Paraguay
- Peru

2. Bonaire, St. Eustatius and Saba

- Puerto Rico
- St. Kitts-Nevis
- St. Lucia
- St. Maarten
- St. Vincent and the Grenadines
- Suriname
- Trinidad and Tobago
- Turks and Caicos Islands
- Uruguay
- Venezuela
- Virgin Islands, British
- Virgin Islands, U.S.

A.5 South Asia/Middle East/Africa Region

The South Asia/Middle East/Africa Region includes the following countries or territories.

- Afghanistan
- Algeria
- Angola
- Bahrain
- Bangladesh
- Benin
- Bhutan
- Botswana
- Bouvet Island
- British Indian Ocean Territory
- Burkina Faso
- Burundi
- Cameroon
- Cape Verde
- Central African Republic
- Chad
- Comoros
- Congo

- Côte D'Ivoire
- Democratic Republic of the Congo
- Djibouti
- Egypt
- Equatorial Guinea
- Eritrea
- Ethiopia
- Gabon
- Gambia
- Ghana
- Guinea
- Guinea-Bissau
- India
- Iraq
- Jordan
- Kenya
- Kuwait
- Lebanon
- Libyan Arab Jamahiriya
- Madagascar
- Malawi
- Maldives
- Mali
- Mauritania
- Mauritius
- Morocco
- Mozambique
- Namibia
- Nepal
- Niger
- Nigeria
- Oman
- Pakistan
- Palestinian Territory, Occupied

- Qatar
- Reunion
- Rwanda
- Sao Tome and Principe
- Saudi Arabia
- Senegal
- Seychelles
- Sierra Leone
- Somalia
- South Africa
- Sri Lanka
- Swaziland
- Syrian Arab Republic
- Tanzania, United Republic of
- Togo
- Tunisia
- Uganda
- United Arab Emirates
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

A.6 United States Region

The United States Region is composed of the United States.

Appendix C Maestro Merchant Operating Guidelines (MOG)—Europe Region Only

C.1 Maestro Merchant Operating Guidelines (MOG)

The information detailed below must be provided by Acquirers to their contracted Merchants and, where appropriate, included in the Merchant contract itself.

C.1.1 General Information

Maestro enables customers to pay for goods and services by electronic means (for example, no paper vouchers).

Maestro supports the purchase and refund of goods and services.

Payment is guaranteed for all successful Transactions undertaken via the POS Terminal in accordance with the Rules.

Cardholder verification may be made by PIN or signature depending on the configuration of the POS Terminal. At dual POS Terminals Cardholder verification must be by PIN.

All staff who accept Cards should be familiar with the Maestro point-of-sale procedures.

C.1.2 Card Recognition and Acceptance

Cards have their own unique identity dependent upon the Issuer. However, Merchants will be able to identify them easily, through the appearance on each Card of the instantly recognizable Maestro logo. The Maestro logo will be found on either the front or the back of the Card.

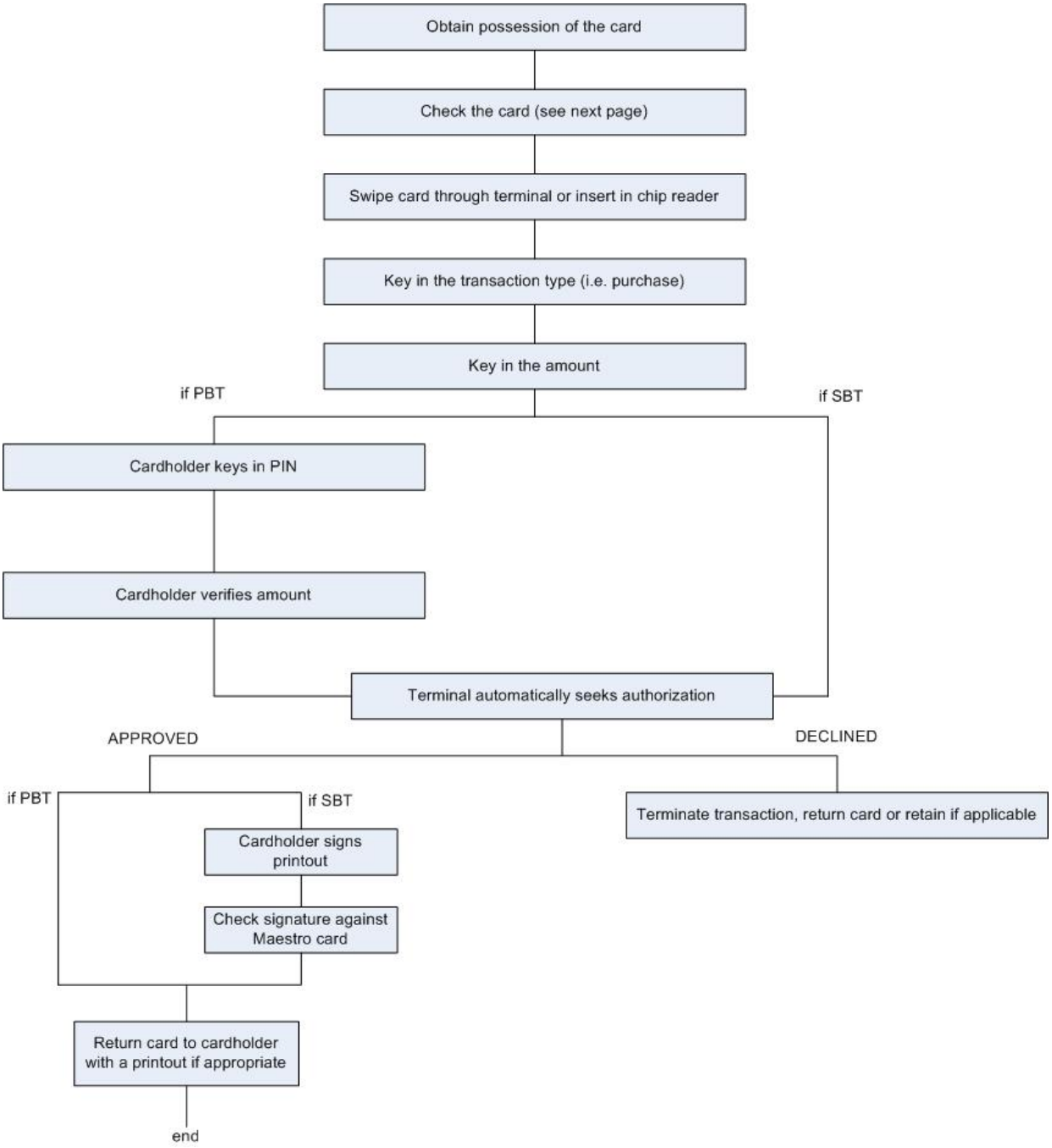
All Cards, when properly presented as payment from customers for Transactions, must be honored without discrimination.

C.1.3 Basic Procedures

As the order in which POS Terminal-related activities are performed may vary according to the type and nature of the POS Terminal, the Acquirer must ensure that its Merchants are provided with the operating procedures relating to the specific POS Terminal installed.

C.1.3.1 Purchase Transactions

The following diagram illustrates the standard purchase Transaction procedure:



C.1.3.2 Refund Transactions

Procedure is similar to that of purchase but with the following difference: if a Maestro receipt is presented as proof of purchase, it should be checked to ensure that the signature, where applicable, is the same as that on the Card.

C.1.4 Suspicious Circumstances (Signature-based Transactions)

In the following circumstances, the security procedures detailed by the Merchant's Acquirer should be followed:

1. Cardholder signature differs from that on Card;
2. name/title on Card does not match Cardholder's name/title;
3. Card not signed; and/or
4. signature stripe has been interfered with, or Card is otherwise damaged.

If there is any reason to be suspicious about the validity of the Card, the Transaction or the person presenting the Card, the Transaction should not be undertaken.

C.1.5 If a Customer Leaves a Card in the Shop

1. It should be kept for forty-eight (48) hours in a safe place.
2. If it is claimed within that time, it must only be handed over once the signature on the Card has been compared with that of the claimant.
3. Cards unclaimed after forty-eight (48) hours must be cut in half through the magnetic stripe and returned to the Acquirer.

Appendix D Signage, Screen, and Receipt Text Displays

D.1 Screen and Receipt Text Standards

Response Code	Recommended Screen Text	Recommended Receipt Text
• Format error • Invalid acquirer • Cardholder not on file • Do not honor/Restricted card • Unable to process/System error • ATM processor inoperative • Cardholder processor inoperative/Not found	"I am sorry. I am unable to process your request. Please contact your financial institution."	"Denied Unable to Process"
• Invalid transaction • Invalid transaction selection	"I am sorry. You have selected an invalid transaction. Do you want to try another transaction?"	"Denied Invalid Transaction"
• Invalid amount	"You have selected an invalid amount. Please select an amount in multiples of ."	"Denied Invalid Amount"
• Insufficient funds	"I am unable to process for insufficient funds. Please contact your financial institution."	"Denied Insufficient Funds"
• Invalid PIN	"You have entered your PIN incorrectly. Do you want to try again?"	"Denied Invalid PIN"
• PIN tries exceed permitted number of attempts	"You have exceeded the number of attempts permitted to enter your PIN. Please contact your financial institution."	"Denied Invalid PIN"
• Exceeds withdrawal limit	"You have exceeded the withdrawal limit. Do you want to select another amount?"	"Denied Invalid Amount"
• Denied—Capture card	"Your card has been retained. Please contact your financial institution."	"Denied Card Retained"

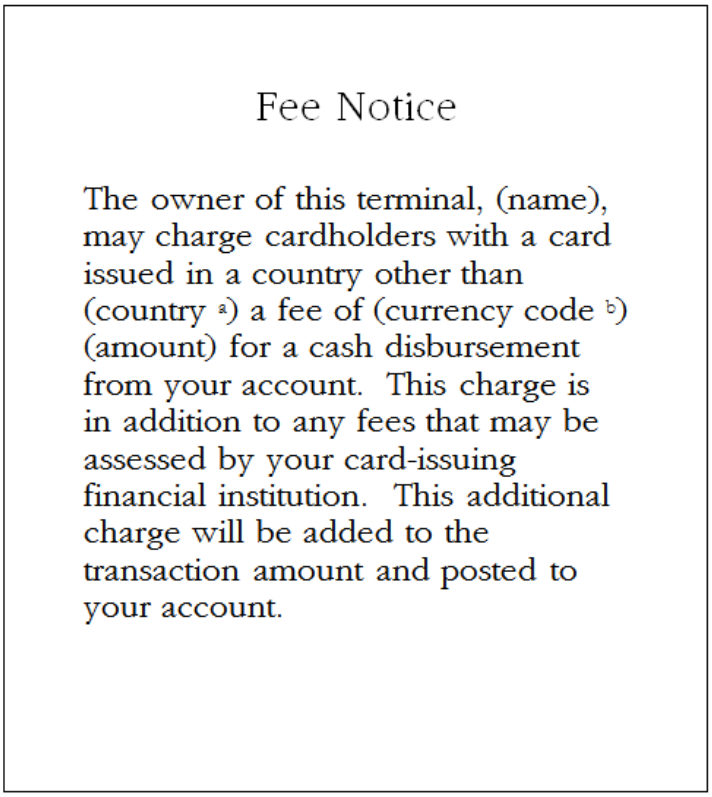
D.2 Model Form for Terminal Signage Notification of ATM Access Fee

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee.

D.2.1 Asia/Pacific Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Asia/Pacific Region, except Australia. For more information about Australia, refer to section D.2.1.1 of this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



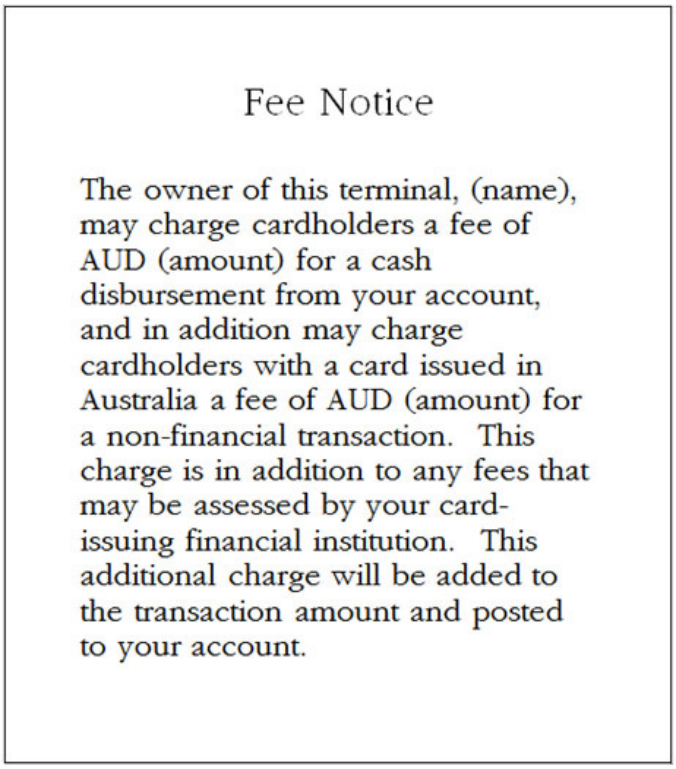
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.2.1.1 Australia

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for Australia only. Use the following dimensions:

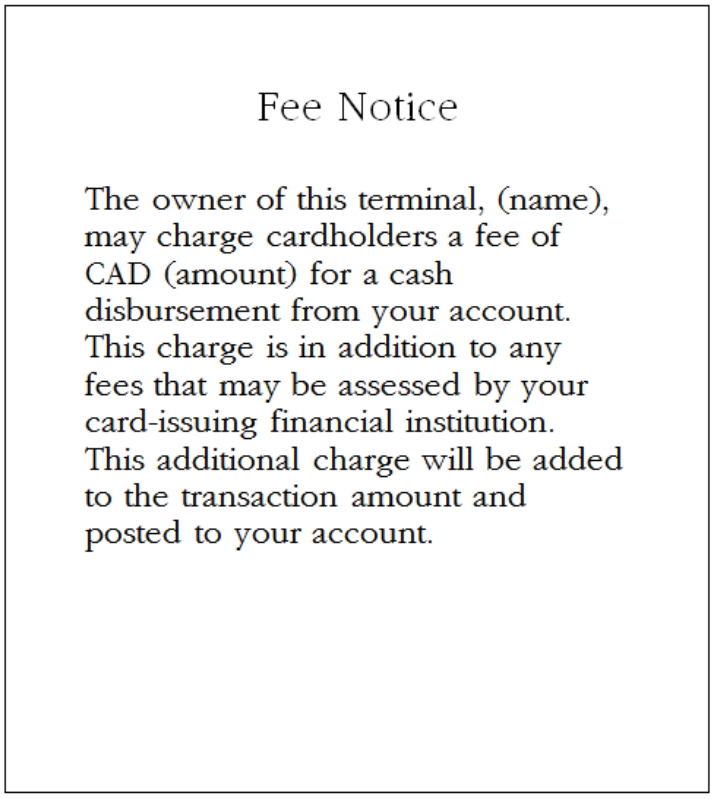
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.2.2 Canada Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Canada Region only. Use the following dimensions.

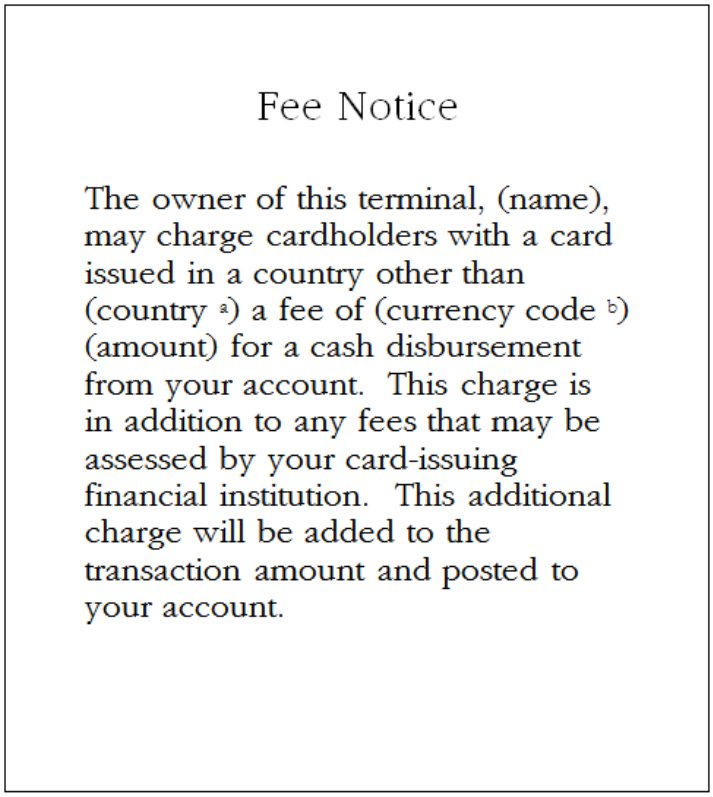
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.2.3 Europe Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Europe Region only, except the United Kingdom. For more information about the United Kingdom, refer to section D.2.3.1 of this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



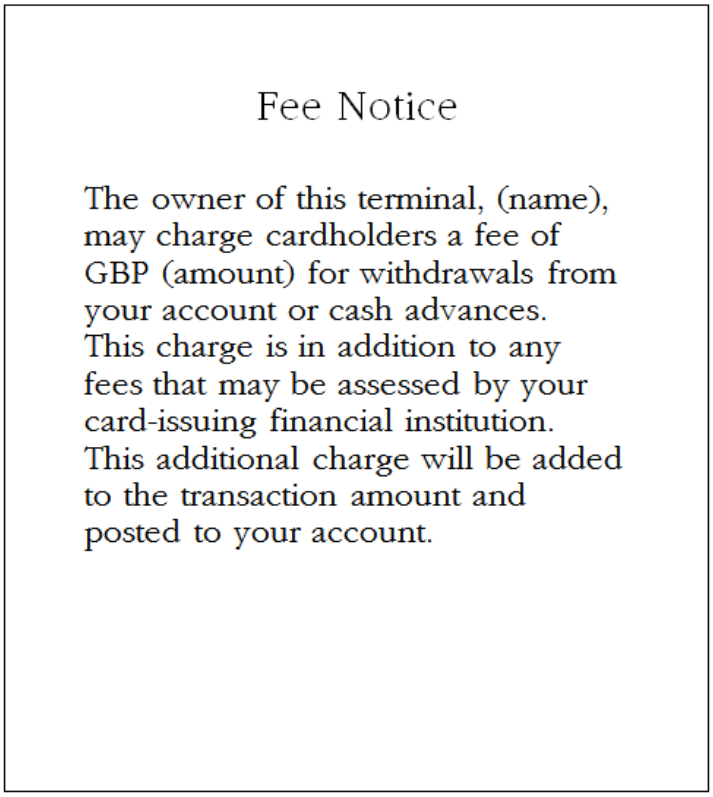
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.2.3.1 United Kingdom

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the United Kingdom only. Use the following dimensions.

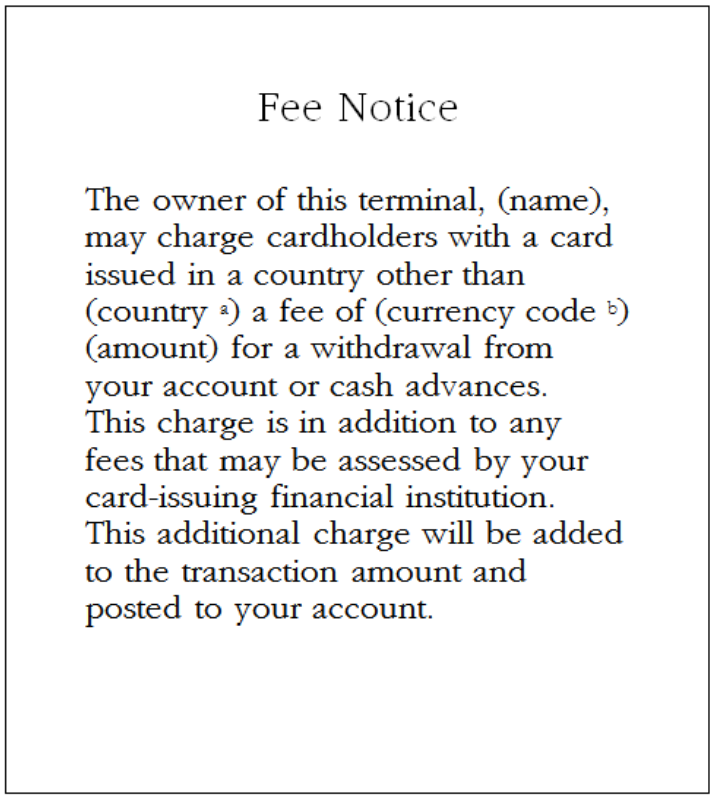
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.2.4 Latin America and the Caribbean Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for Latin America and the Caribbean Region except the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela. For more information about Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela, refer to section D.2.4.1 in this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



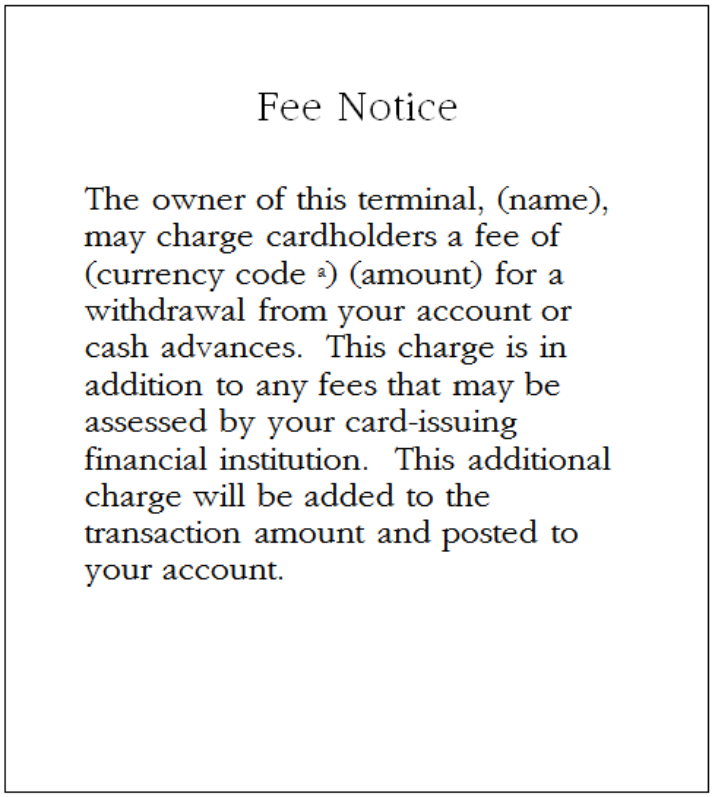
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.2.4.1 Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for only the following countries in the Latin America and the Caribbean Region: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.

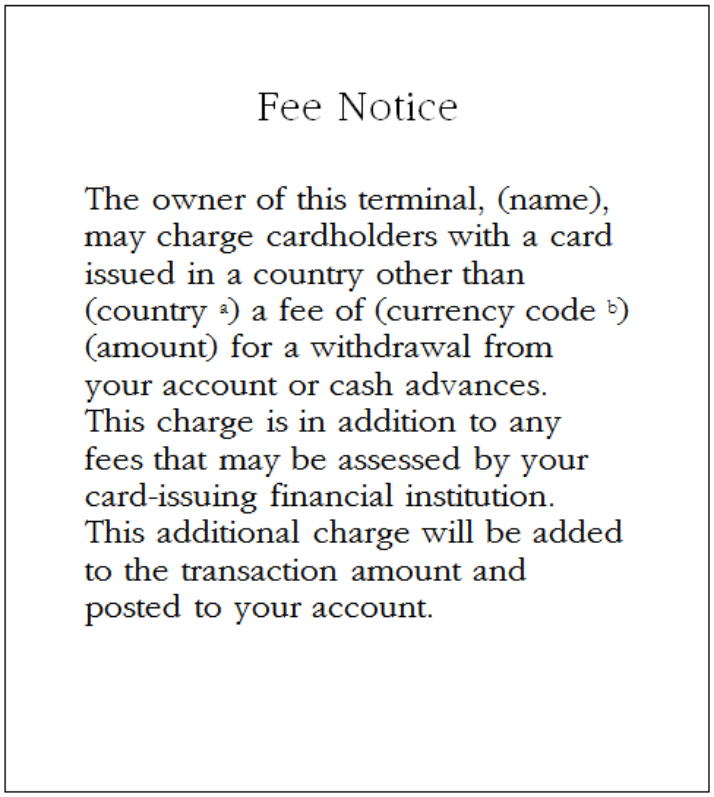


a Insert currency code for the country where the ATM is located. Argentina (ARS), Brazil (BRL), Chile (CLP), Colombia (COP), Ecuador (USD), Mexico (MXN or MXV), Panama (PAB or USD), Peru (PEN), Puerto Rico (USD), or Venezuela (VEB).

D.2.5 South Asia/Middle East/Africa Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the South Asia/Middle East/Africa Region. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



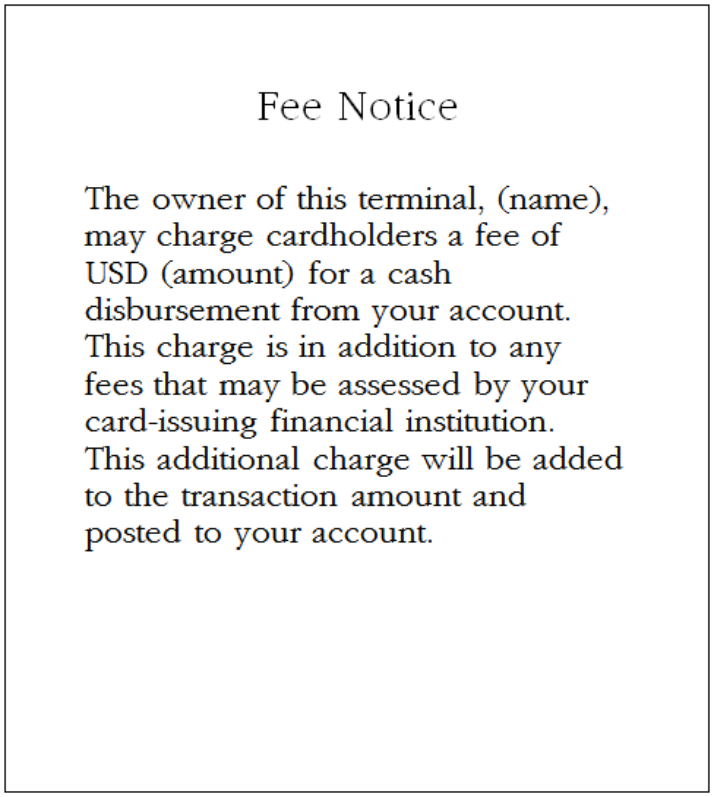
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.2.6 United States Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the United States only. Use the following dimensions.

Object	Dimension
Screen height	Minimum of four (4) inches
Screen width	Minimum of four (4) inches
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



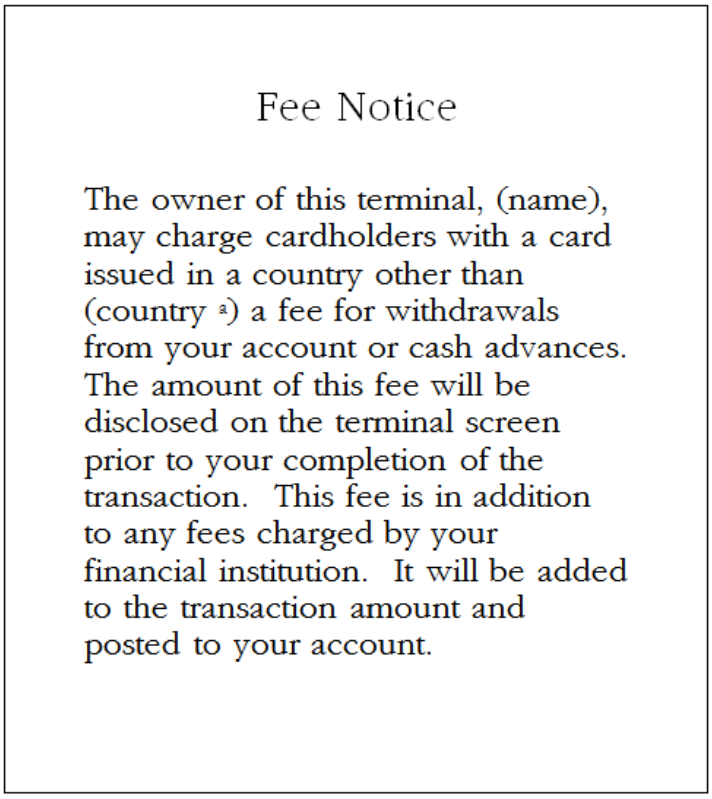
D.3 Model Form for Generic Terminal Signage Notification of ATM Access Fee

The following model form illustrates dimensions for Terminal signage notification.

D.3.1 Asia/Pacific Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Asia/Pacific Region, except Australia. For more information about Australia, refer to section D.3.1.1 of this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.

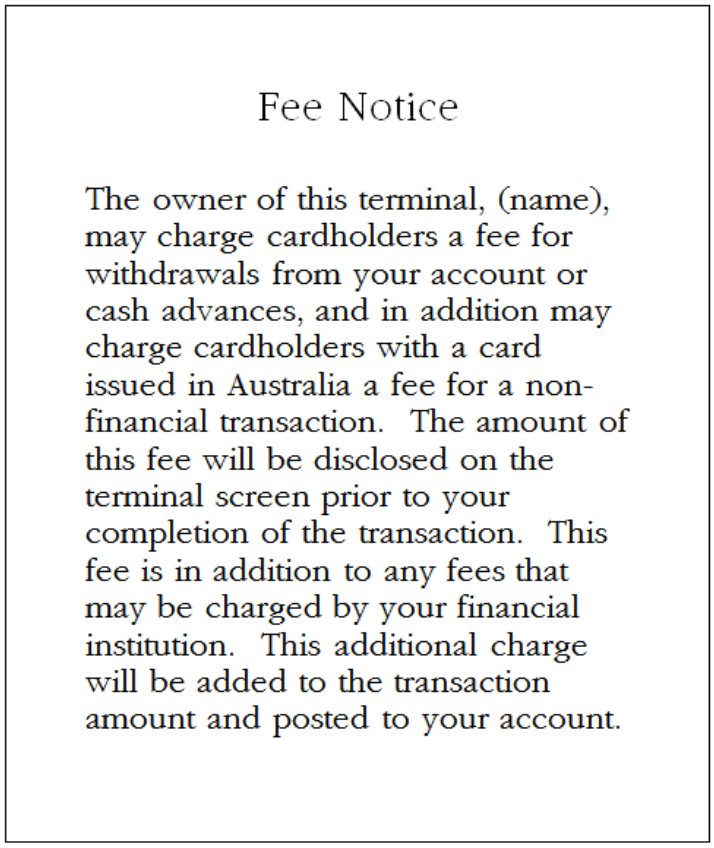


a Insert country where ATM is located.

D.3.1.1 Australia

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for Australia only. Use the following dimensions.

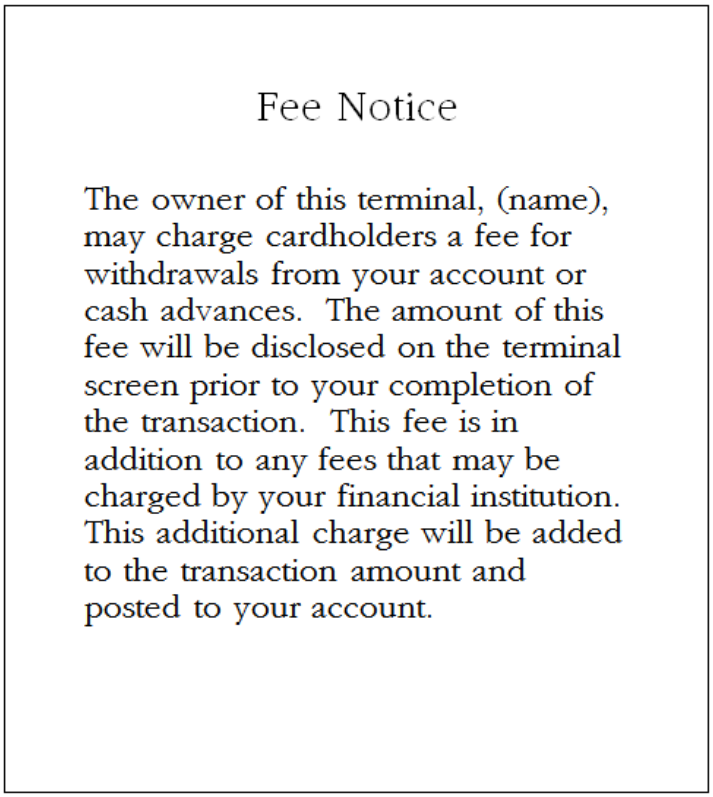
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.3.2 Canada Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Canada Region only. Use the following dimensions.

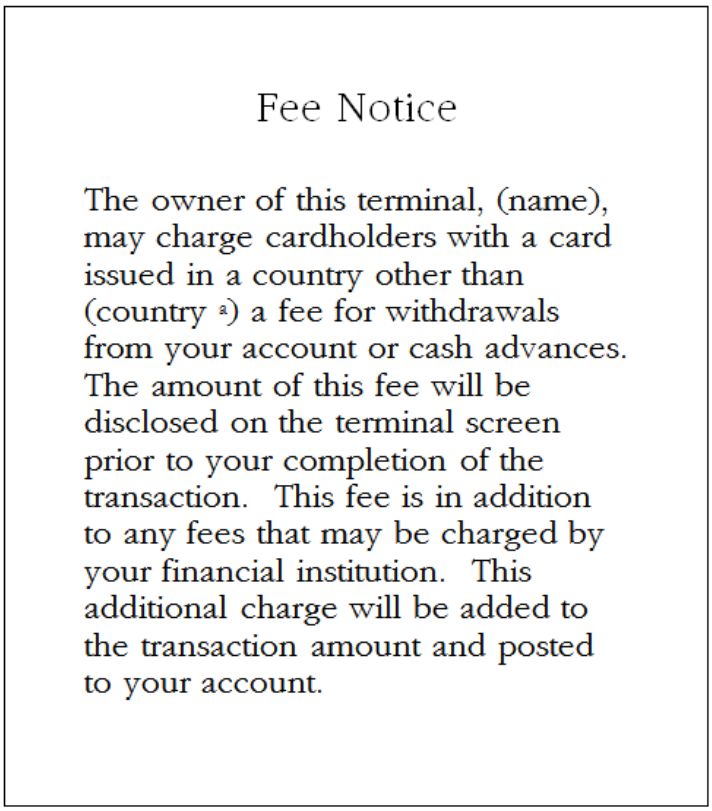
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.3.3 Europe Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Europe Region only, except the United Kingdom. For more information about the United Kingdom, refer to section D.3.3.1 of this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.

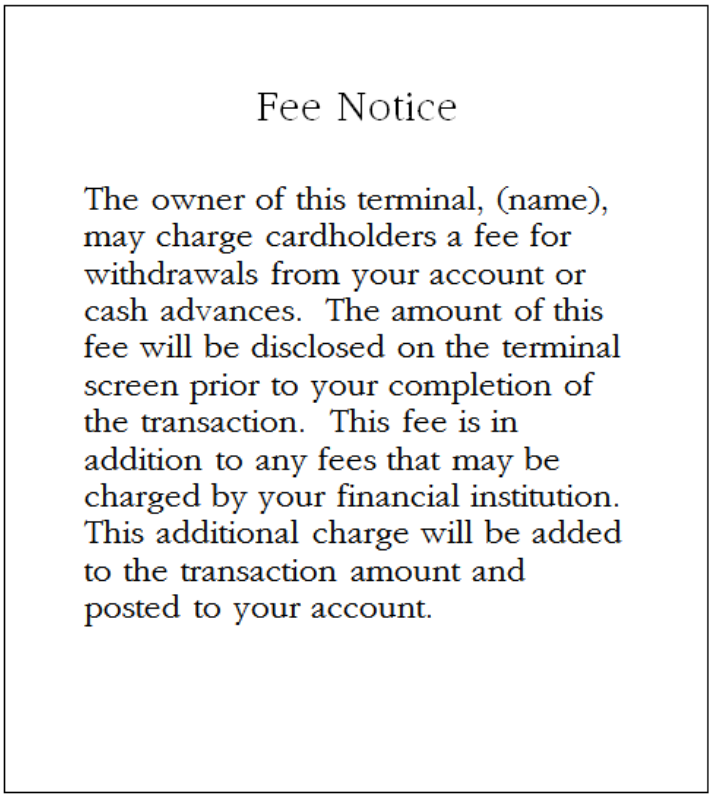


a Insert country where ATM is located.

D.3.3.1 United Kingdom

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the United Kingdom only. Use the following dimensions.

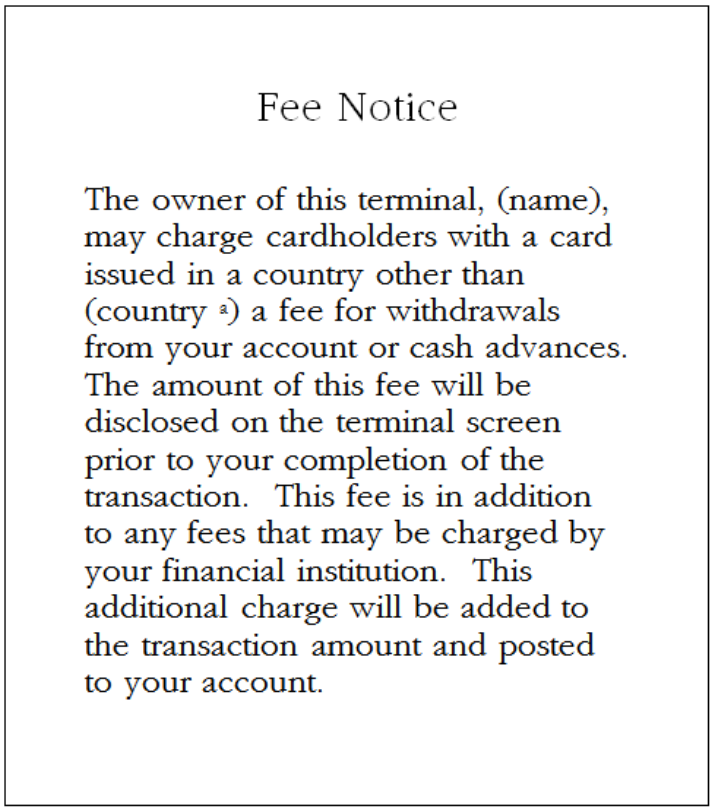
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.3.4 Latin America and the Caribbean Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for Latin America and the Caribbean Region except the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela. For more information about Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela, refer to section D.3.4.1 in this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.

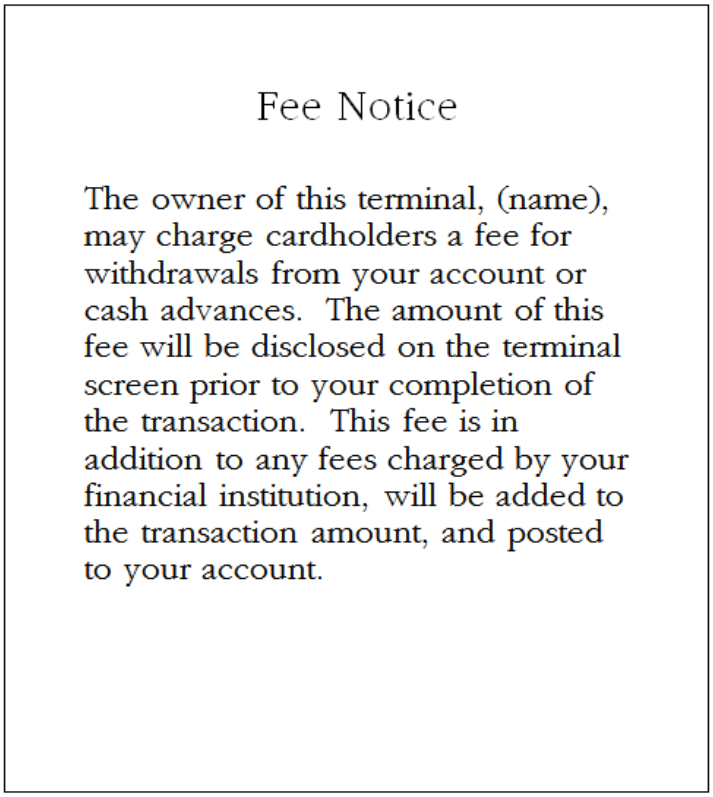


a Insert country where ATM is located.

D.3.4.1 Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for only the following countries in the Latin America and the Caribbean Region: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela. Use the following dimensions.

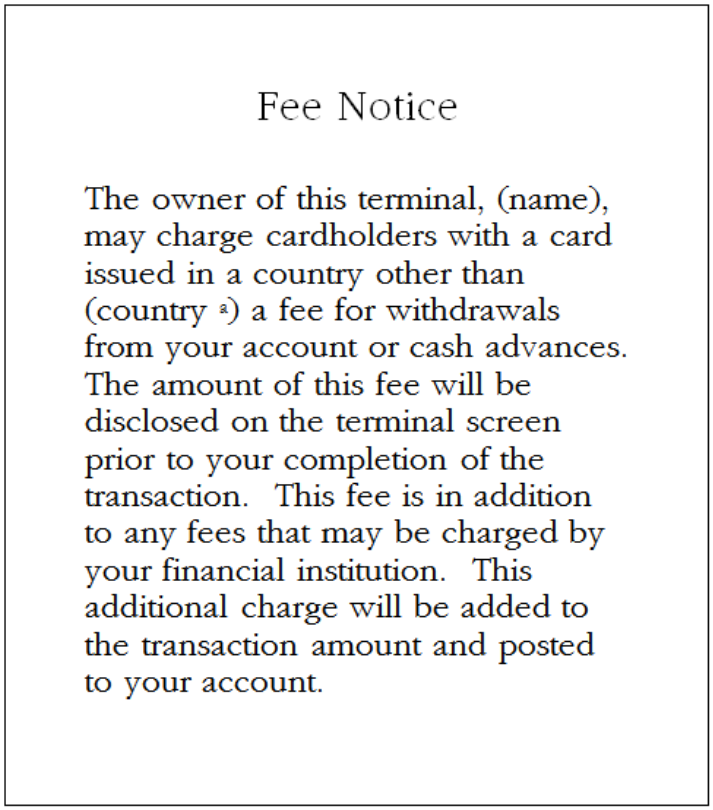
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.3.5 South Asia/Middle East/Africa Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the South Asia/Middle East/Africa Region. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.

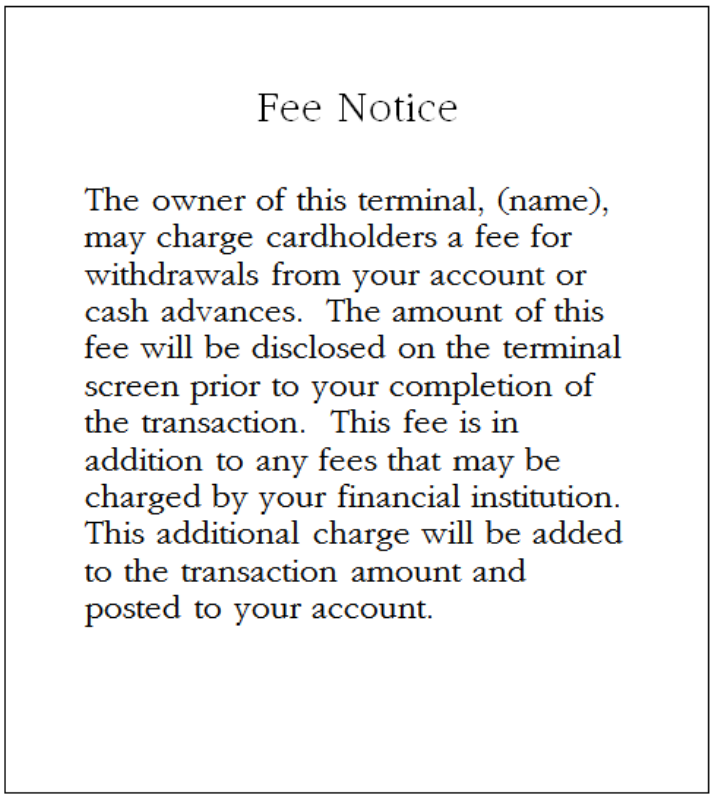


a Insert country where ATM is located.

D.3.6 United States Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the United States only. Use the following dimensions.

Object	Dimension
Screen height	Minimum of four (4) inches
Screen width	Minimum of four (4) inches
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

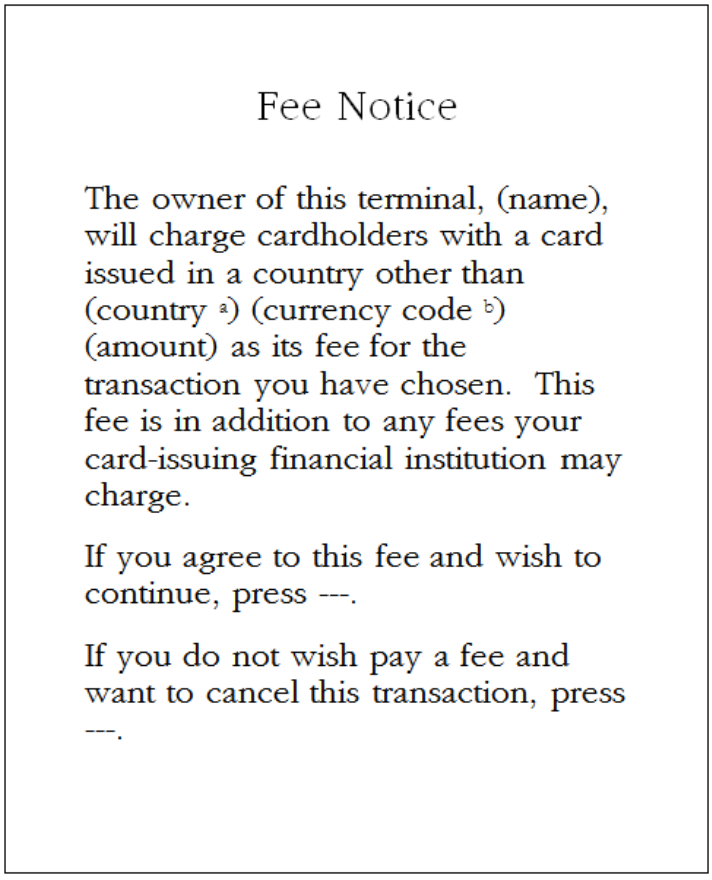
D.4 Model Form for Screen Display Notification of ATM Access Fee

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee.

D.4.1 Asia/Pacific Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Asia/Pacific Region, except Australia. For more information about Australia, refer to section D.4.1.1 in this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



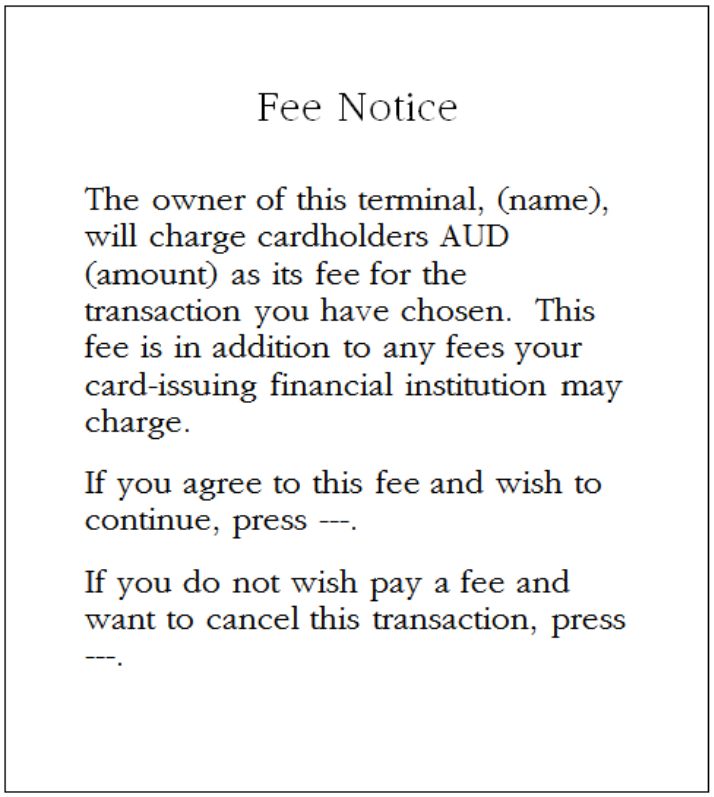
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.4.1.1 Australia

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for Australia only. Use the following dimensions.

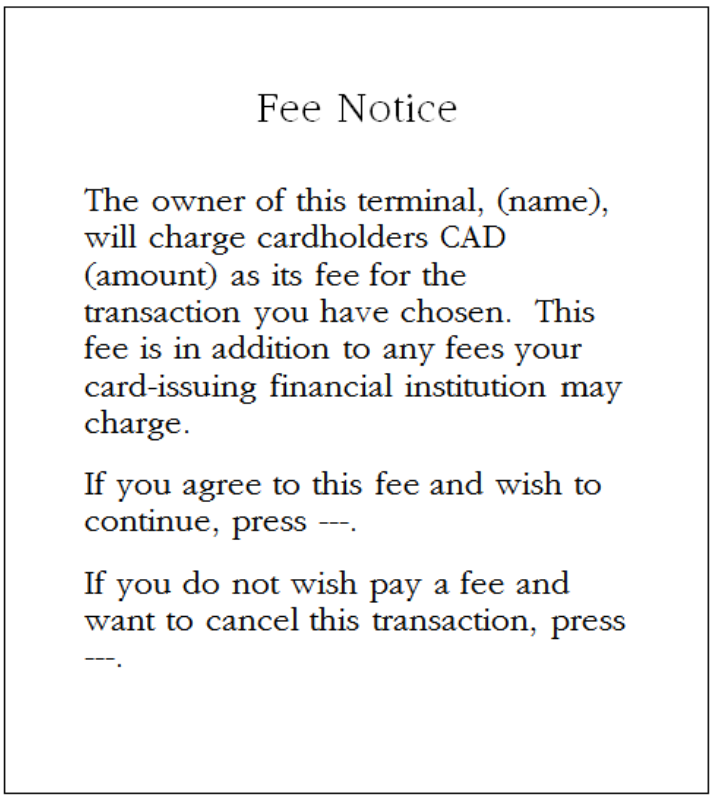
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.4.2 Canada Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for Canada only. Use the following dimensions.

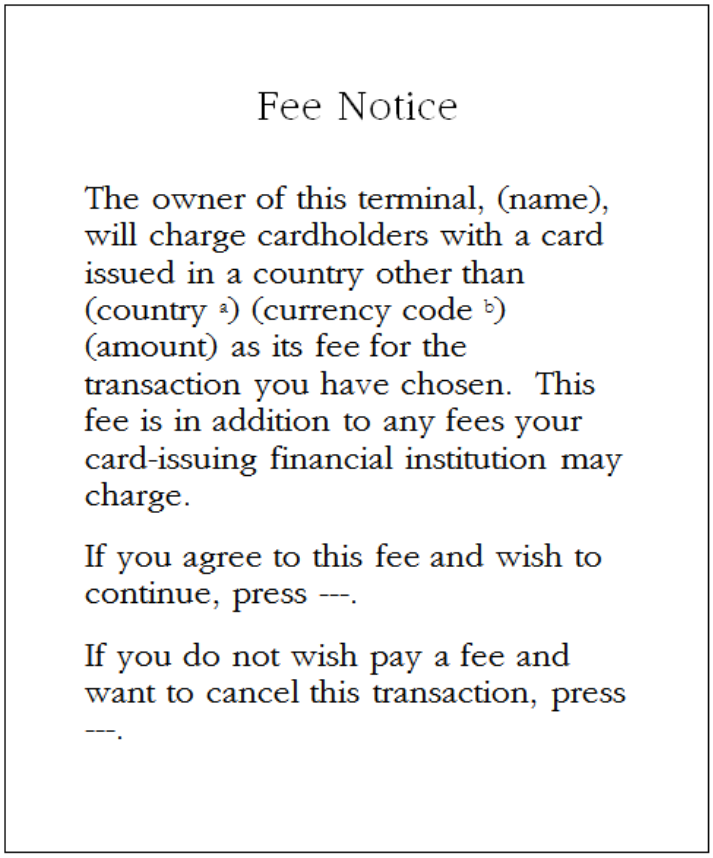
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.4.3 Europe Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Europe Region, except the United Kingdom. For more information about the United Kingdom, refer to section D.4.3.1 in this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



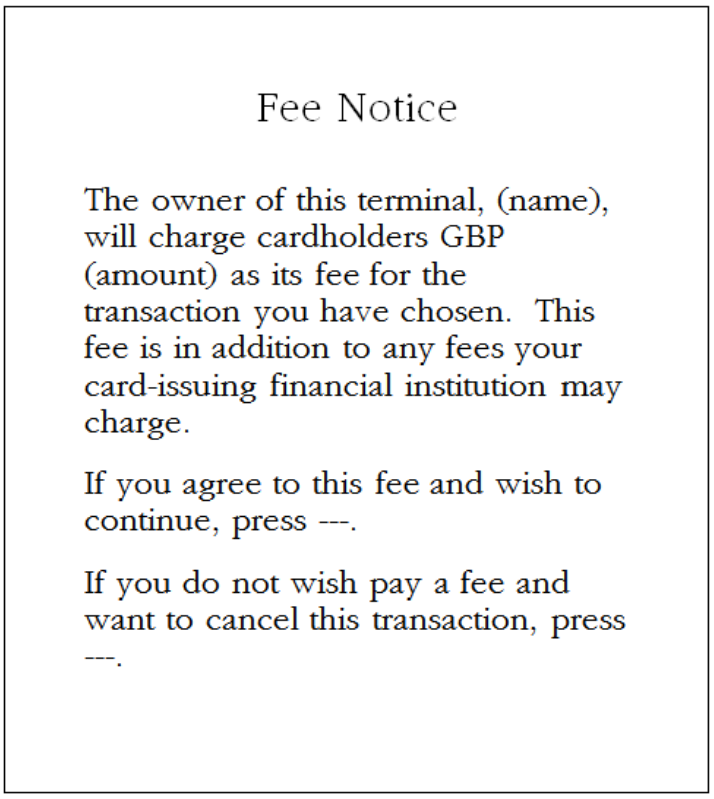
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.4.3.1 United Kingdom

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for United Kingdom only. Use the following dimensions.

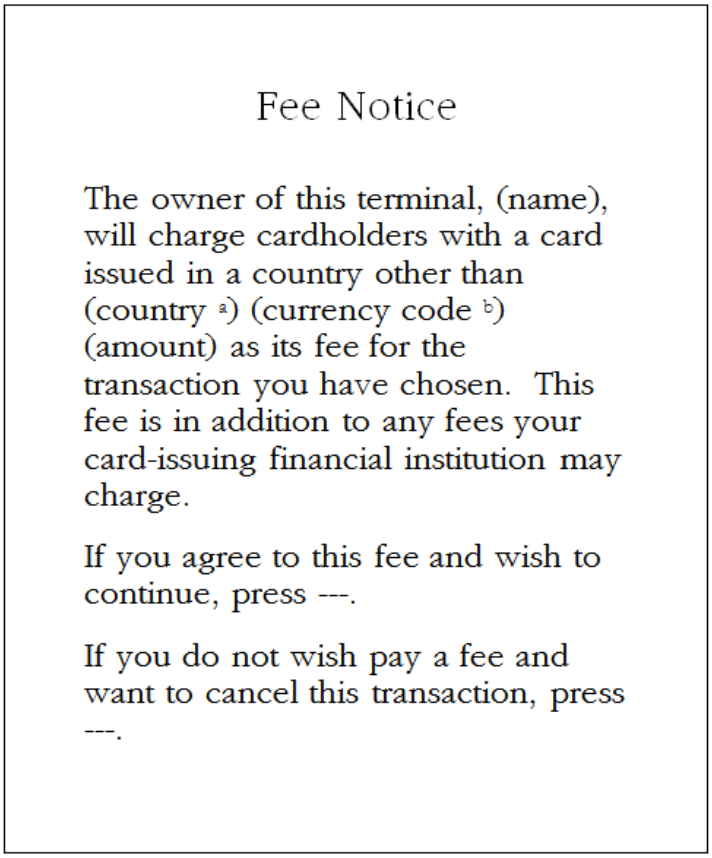
Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.4.4 Latin America and the Caribbean Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the Latin America and the Caribbean Region except the following countries: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela. For more information about Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela, refer to section D.4.4.1 in this rulebook. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



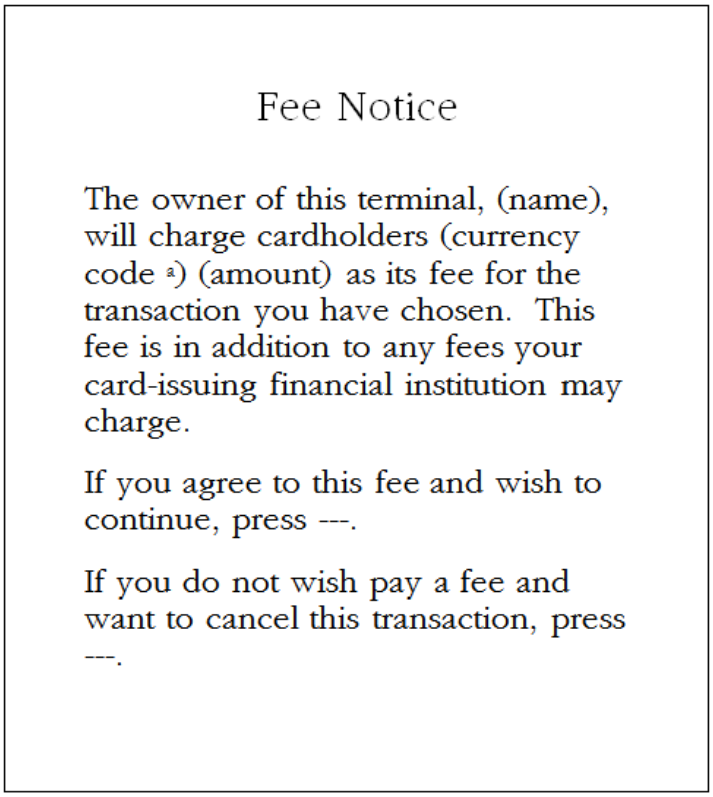
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.4.4.1 Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for only the following countries in the Latin America and the Caribbean Region: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Panama, Peru, Puerto Rico, and Venezuela. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.

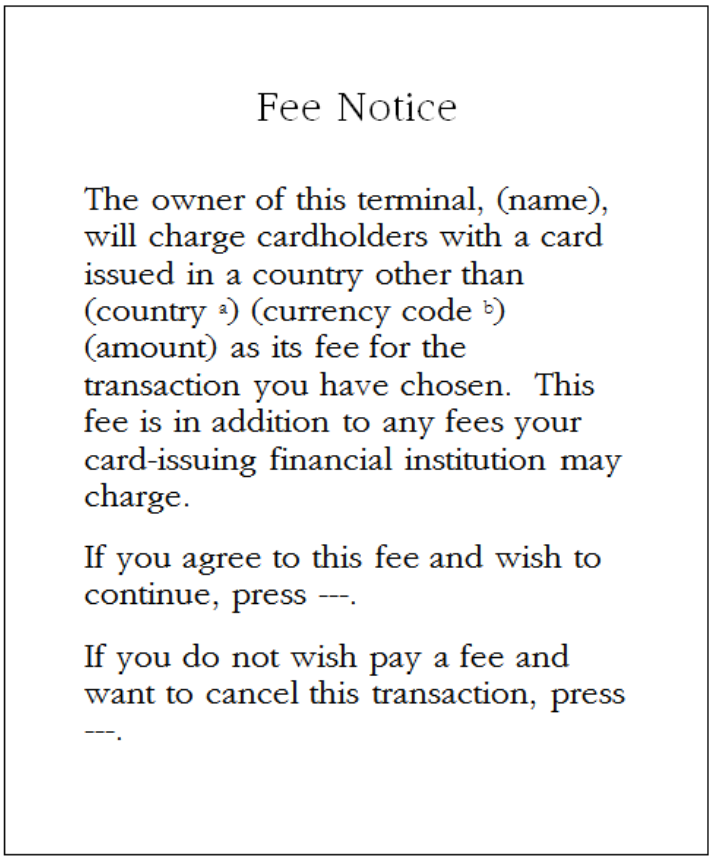


a Insert currency code for the country where the ATM is located: Argentina (ARS), Brazil (BRL), Chile (CLP), Colombia (COP), Ecuador (USD), Mexico (MXN or MXV), Panama (PAB or USD), Peru (PEN), Puerto Rico (USD), or Venezuela (VEB).

D.4.5 South Asia/Middle East/Africa Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for the South Asia/Middle East/Africa Region. Use the following dimensions.

Object	Dimension
Screen height	Minimum of ten (10) centimeters
Screen width	Minimum of ten (10) centimeters
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



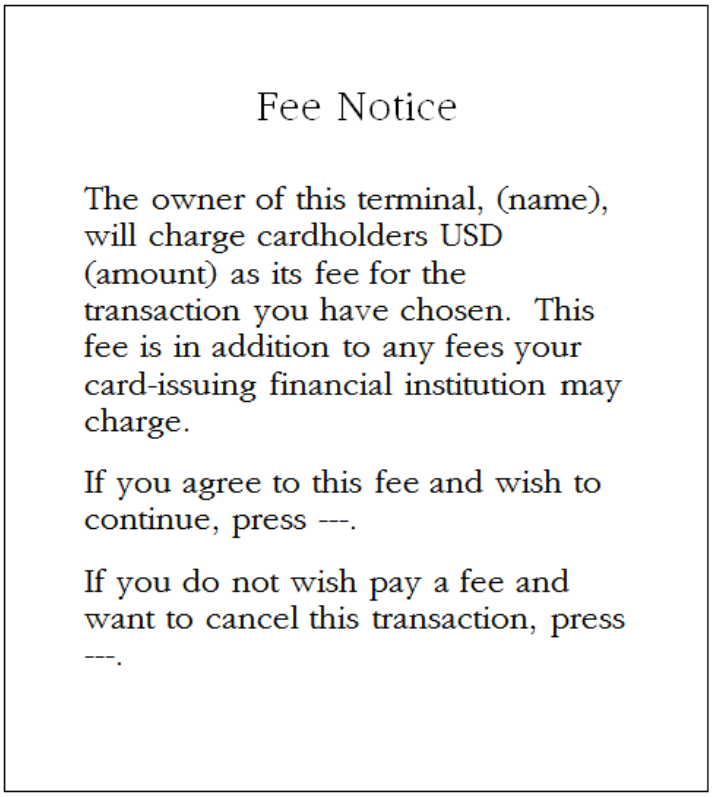
a Insert country where ATM is located.

b Insert currency code for the country where the ATM is located.

D.4.6 United States Region

The following model form illustrates dimensions for Terminal signage notification of ATM Access Fee for United States only. Use the following dimensions.

Object	Dimension
Screen height	Minimum of four (4) inches
Screen width	Minimum of four (4) inches
Heading text	Must be at least 18 point type.
Body text	Must be at least 14 point type.



D.5 Model Form for ATM Access Fee Transaction Receipt

$100.00	Paid to Cardholder
$ 1.00	Terminal Owners Fee
$101.00	Withdrawal from checking

D.6 Model Screens Offering POI Currency Conversion

Option A, Screen 1

YOU MAY PAY FOR THIS TRANSACTION IN YOUR HOME CURRENCY.

CASH WITHDRAWAL	GBP 50.00
ACCESS FEE	GBP 1.50
TOTAL AMOUNT	GBP 51.50
TERMINAL EXCHANGE RATE	GBP 1.00 = EUR 1.25
TRANSACTION AMOUNT	EUR 64.38
<<< CHARGE MY ACCOUNT GBP 51.50	CHARGE MY ACCOUNT EUR 64.38 >>>

Screen 2

(Statement and screen may be varied or omitted subject to the agreement of the Corporation.)

I HAVE CHOSEN NOT TO USE THE MASTERCARD CURRENCY CONVERSION PROCESS AND I WILL HAVE NO RECOURSE AGAINST MASTERCARD CONCERNING THE CURRENCY CONVERSION OR ITS DISCLOSURE.

<<< PROCEED WITH CONVERSION RETURN TO PREVIOUS SCREEN >>>

Option B, Screen 1

THIS TERMINAL OFFERS CONVERSION TO YOUR HOME CURRENCY.

CASH WITHDRAWAL	GBP 50.00
ACCESS FEE	GBP 1.50
TOTAL AMOUNT	GBP 51.50
TERMINAL EXCHANGE RATE	GBP 1.00 = EUR 1.25
TRANSACTION AMOUNT WITH CONVERSION	EUR 64.38
	CONTINUE WITH CONVERSION >>>
	CONTINUE WITHOUT CONVERSION >>>

Screen 2

(Statement and screen may be varied or omitted subject to the agreement of the Corporation.)

I HAVE CHOSEN NOT TO USE THE MASTERCARD CURRENCY CONVERSION PROCESS AND I WILL HAVE NO RECOURSE AGAINST MASTERCARD CONCERNING THE CURRENCY CONVERSION OR ITS DISCLOSURE.

<<< PROCEED WITH CONVERSION RETURN TO PREVIOUS SCREEN >>>

D.7 Model Receipt for Withdrawal Completed with POI Currency Conversion

CASH WITHDRAWAL	GBP 50.00
ACCESS FEE	GBP 1.50
TOTAL AMOUNT	GBP 51.50
TERMINAL EXCHANGE RATE	GBP 1.00 = EUR 1.25
TRANSACTION AMOUNT	EUR 64.38

(The following statement may be varied or omitted subject to the agreement of the Corporation.)

I have chosen not to use the MasterCard currency conversion process and I will have no recourse against MasterCard concerning the currency conversion or its disclosure.

D.8 Recommended Screen Messages—Europe Region Only

The following texts in Dutch, English, French, German, Italian, and Spanish are the recommended screen messages for use on Terminals.

D.8.1 Correspondence Host-EM Response Code/Terminal Messages Screen Messages

The following table lists proposed screen message related to the response code received:

Host-EM Response Code	Terminal Messages
00	1
01	2
04	9

Host-EM Response Code	Terminal Messages
05	7
12	7
13	5
14	9
30	11
33	8
36	7
38	4
41	9
43	9
51	6
54	8
55	3
61	5
75	4
76	9

D.8.2 Messages for Cardholders and Cashiers in English and Local Language

Message Number	Cardholder Message(in English)	Cashier Message(in Local Language)
1	Transaction ok	Transaction approved—Dispense requested amount and return card
2	Enter your PIN	Enter PIN
3	Retry PIN	Retry PIN
4	Wrong PIN	Wrong PIN—Cancel transaction and return card
5	Try lower amount	Try lower amount
6	No funds	Insufficient funds—Return card
7	Function not ok	Card not valid for this function—Return card

Message Number	Cardholder Message(in English)	Cashier Message(in Local Language)
8	Card expired	Retain card for security reasons—Do not return card
9	Card not valid	Machine failure—Return card
10	Machine failure	Time out—Return card
11	System problems	Time out—Return card
12	Please wait	Please wait

D.9 ATMs—Europe Region Only

D.9.1 Correspondence Host-EM Response Code/Terminal Messages Screen Messages

D.9.1 Correspondence Host-EM Response Code/Terminal Messages Screen Messages

Host-EM Response Code	Screen Messages
00	6
01	16
04	12
05	16
12	1 or 13
13	5 or 13
14	13
30	13
33	12
36	16
38	12
41	12
43	12
51	5 or 13
54	11
55	3

Host-EM Response Code	Screen Messages
61	5 or 13
75	8
76	8

D.9.2 Messages for Cardholders

D.9.2.1 Messages in Dutch

The following table lists single line screen messages in Dutch:

ID	Message Text
1	Kaart ongeldig vr internationaal gebruik
2	Toets uw codenummer in a.u.b.
3	Fout codenummer, probeer nogmaals a.u.b.
4	Welk bedrag wenst u? Max. XXXXXX CCCC
5	Het bedrag is XXXXXX, u kan veranderen
6	Neem uw biljetten a.u.b.
7	Neem uw kaart terug a.u.b.
8	Te veel onjuiste codenummers
9	Transactie afgebroken. Te lang gewacht
10	Kaart beschadigd. Neem ze terug a.u.b.
11	Kaart vervallen. Neem ze terug a.u.b.
12	Kaart ingehouden om veiligheidsredenen
13	Kaart ingehouden. Te lang gewacht
14	Technisch defect. Neem uw kaart terug
15	Technisch defect. Kaart werd ingehouden
16	Kaart teruggegeven om veiligheidsredenen
17	Even geduld a.u.b.
18	Deze automaat is tijdelijk defect

The following table lists full screen messages in Dutch:

ID	Message Text
1	Uw kaart is niet geldig voor internationaal gebruik
2	Toets uw codenummer in. Indien u een fout maakt, druk dan op de gele toets
3	Onjuist codenummer. Probeer nogmaals a.u.b.
4	Hoeveel pesetas wenst u? Maximum 20,0002,0005,00010,00015,00020,000ANDER BEDRAG
5A	Deze automaat geeft enkel biljetten die een veelvoud zijn van 1,000 ptas. Gelieve het gewenste bedrag in te geven en op de groene toets te drukken. Indien u een fout maakt, druk dan op de gele toets
5B	Wij kunnen u het gevraagde bedrag niet in een keer verstrekken. Gelieve een kleiner bedrag in te toetsen
5C	Gelieve een kleiner bedrag in te toetsen. Het maximum toegelaten bedrag is xxx,xxx ptas
5D	Wij beschikken enkel over bankbiljetten van 1,000 en 5,000 ptas. Gelieve een bedrag op te vragen dat met deze biljetten verstrekt kan worden
5E	Op dit ogenblik beschikken wij enkel over bankbiljetten van 5,000 ptas. Gelieve een bedrag op te vragen dat u met deze biljetten verstrekt kan worden
5F	Deze automaat heeft geen bankbiljetten meer. Zie informatie over de dichtstbijgelegen automaat
5G	Onjuiste informatie ingegeven. Probeer nogmaals a.u.b.
6	Neem u ticket en uw geld a.u.b.
7	Neem uw kaart terug a.u.b.
8	Te veel onjuiste codenummers. Uw kaart kan niet langer in geldautomaten gebruikt worden
9A	Gelieve de informatie sneller in te toetsen
9B	De transactie werd afgebroken. Neem uw ticket en uw kaart a.u.b.
10	Uw kaart is niet geldig voor gebruik in <ATM-network> automaten
11	Uw kaart is niet meer geldig. Neem ze terug en vraag uw bank om vervanging
11A	Deze kaart is nog niet geldig
12	Wij kregen opdracht uw kaart in te houden. Vraag uw bank om informatie
13	De transactie werd afgebroken. Neem uw ticket a.u.b.
14A	De automaat is defect. De transactie werd afgebroken. Neem uw kaart terug a.u.b.

ID	Message Text
14B	De automaat is defect. De transactie werd afgebroken. Neem uw ticket en uw kaart a.u.b.
15	Uw kaart werd ingehouden. Gelieve zich tot dit bankagentschap te wenden tijdens kantooruren
16	Wij kregen opdracht uw kaart terug te geven. Gelieve uw bank te contacteren om informatie te vragen
17	Even geduld a.u.b.
18A	Deze automaat is tijdelijk defect. Zie informatie over de dichtstbijgelegen automaat
18B	Deze automaat is defect. Zie informatie over de dichtstbijgelegen automaat
18C	Deze dienst is momenteel niet beschikbaar. Wij verontschuldigen ons hiervoor

D.9.2.2 Messages in English

The following table lists single line screen messages in English:

ID	Message Text
1	Card not valid internationally
2	Please enter your personal number
3	Wrong personal number, please try again
4	Please enter amount, up to XXXXXX CCCC
5	Edited amount XXXXXX, change if needed
6	Please take your money
7	Please take back your card
8	Too many entries of personal number
9	Transaction cancelled, waited too long
10	Your card is faulty. Please take it back
11	Card has expired. Please take it back
12	Card is retained for security reasons
13	Card is retained. You waited too long
14	Machine failure, please take card back
15	Machine failure, card is retained
16	Card returned for security reasons

ID	Message Text
17	Please wait
18	This machine is out of order

The following table lists full screen messages in English:

ID	Message Text
1	Your card is not valid for international withdrawals
2	Enter your personal number. If you made a mistake, press the yellow key
3	Incorrect personal number. Please try again.
4	How many ptas do you require? Maximum 20,000 2,000 5,000 10,000 15,000 20.000 OTHER AMOUNTS
5A	This machine dispenses notes in multiples of 1,000 ptas only. Please enter the amount required and then press the green key. If you made a mistaken press the yellow key.
5B	We cannot give you the amount requested in one operation. Please request a smaller amount.
5C	Please request a smaller amount. The maximum permitted withdrawal is xxx,xxx ptas.
5D	We can only dispense 1,000 and 5,000 ptas notes. Please enter an amount which can be dispensed using these notes.
5E	At present we only have 5,000 ptas notes. Please enter an amount which can be dispensed using these notes.
5F	We have run out of notes. See notice indicating location of nearest alternative machine.
5G	Incorrect entry. Please try again.
6	Please take your receipt and your money.
7	Please take your card.
8	Too many wrong personal number entries. Your card can no longer be used in cash dispenses. Please remove and ask your bank for a replacement.
9A	Please enter information more quickly.

ID	Message Text
9B	Transaction cancelled. Please take your card and your receipt.
10	Your card is not valid for use in <ATM network> machines.
11	Your card is out of date. Please take it and ask your bank for a replacement.
12	We have been instructed to withdraw the card.Please contact your own bank for information.
13	Transaction cancelled.Please take your receipt.
14A	Machine out of order. Transaction cancelled. Please take your card.
14B	Machine out of order. Transaction cancelled. Please take your receipt and your card.
15	Card retained for assistance. Please call into this branch during office hours.
16	We have been instructed to return the card.Please contact your own bank for information.
17	Please wait.
18A	This machine is temporarily out of order. See notice indicating location of nearest alternative machine.
18B	This machine is out of order. See notice indicating location of nearest alternative machine.
18C	The service is not available at present. We apologize for any inconvenience.

D.9.2.3 Messages in French

The following table lists single line screen messages in French:

ID	Message Text
1	Carte non valable à l'étranger
2	Composez votre code secret svp
3	Code secret incorrect. Retapez svp
4	Entrez le montant jusqu'à XXXXXX CCC
5	Montant corrigé XXXXXX, on peut changer
6	Prenez votre argent svp
7	Reprenez votre carte svp
8	Trop d'entrées du code secret

ID	Message Text
9	Transaction annulée. Trop d'attente
10	Carte défectueuse. Reprenez-la svp
11	Carte expirée. Reprenez-la svp
12	Carte retenue pour raison de sécurité
13	Carte retenue. Trop d'attente
14	Machine défectueuse, reprenez la carte svp
15	Machine défectueuse, carte retenue
16	Carte rendue pour raison de sécurité
17	Un instant s'il vous plaît
18	Hors service

The following table lists full screen messages in French:

ID	Message Text
1	Votre carte n'est pas acceptée sur le réseau international.
2	Composez votre numéro de code. En cas d'erreur, appuyez sur la touche jaune.
3	Ce numéro de code est incorrect. Recommencez s'il vous plait.
4	Choisissez le montant Maximum 20,000 ptas 2,000 5,000 10,000 15,000 20,000 AUTRES MONTANTS
5A	Cet appareil distribue des billets par multiples de 1,000 ptas. Introduisez le montant et appuyez sur la touche verte. En cas d'erreur, appuyez sur la touche jaune.
5B	Ce montant ne peut être retiré en une seule opération. Veuillez demander une somme plus petite.
5C	Les retraits sont limités a xxx,xxx ptas par jour. Veuillez demander une somme plus petite.
5D	Cet appareil ne distribue que des billets de 1,000 et 5,000 ptas. Introduisez un montant compatible s'il vous plait.

ID	Message Text
5E	Actuellement cet appareil ne dispose que de billets de 5,000 ptas. Introduisez un montant compatible s'il vous plait.
5F	Réserve de billets de banque épuisée. Consultez le panneau indiquant l'appareil le plus proche.
5G	Opération incorrecte. Recommencez s'il vous plait.
6	Votre retrait est accepté. Voici votre reçu et l'argent demande.
7	Reprenez votre carte s'il vous plait.
8	Trop d'entrées du code secret. Votre carte ne peut plus être utilisée dans les guichets automatiques. Reprenez votre carte svp et voyez votre banque pour la renouveler.
9A	Effectuez votre opération plus rapidement, s'il vous plait.
9B	Votre opération est annulée. Reprenez votre reçu et votre carte, s'il vous plait.
10	Votre carte ne peut plus être utilisée sur les appareils du réseau <ATM-network>.
11A	Votre carte n'est plus valable. Reprenez votre carte et voyez votre banque pour la renouveler.
11B	Cette carte ne peut pas encore être utilisée.
12	Votre carte doit être retenue. Consultez votre banque, s'il vous plait.
13	L'opération est annulée. Prenez votre reçu svp.
14A	Cet appareil est hors service. L'opération est annulée. Reprenez votre carte, s'il vous plait.
14B	Cet appareil est hors service. L'opération est annulée. Prenez votre reçu et votre carte, s'il vous plait.
15	Carte retenue. Adressez-vous au guichet de cette agence pour la récupérer.
16	Votre carte vous est restituée. Veuillez vous adresser à votre banque pour toute information.
17	Un instant s'il vous plait. Votre demande est examinée.
18A	Temporairement hors service. Consultez le panneau indiquant l'appareil le plus proche.
18B	Hors service. Consultez le panneau indiquant l'appareil le plus proche.
18C	Le service n'est pas disponible pour l'instant. Veuillez nous excuser des désagréments causes.

D.9.2.4 Messages in German

The following table lists single line screen messages in German:

ID	Message Text
1	Karte international ungültig
2	Bitte Geheimzahl eingeben
3	Geheimzahl falsch, bitte neu eingeben
4	Bitte Betrag eingeben bis zu XXXXXX CCC
5	Betrag geändert auf XXXXXX, korrigierbar
6	Bitte Geld entnehmen
7	Bitte Karte entnehmen
8	Zu viele falsche Eingaben der Geheimzahl
9	Vorgang abgebrochen. Zeitüberschreitung
10	Karte fehlerhaft. Bitte entnehmen
11	Karte verfallen. Bitte entnehmen
12	Karte aus Sicherheitsgründen einbehalten
13	Zeitüberschreitung. Karte einbehalten
14	Maschinenfehler, bitte Karte entnehmen
15	Maschinenfehler. Karte wurde einbehalten
16	Karte w. Sicherheitsgründen zurückgegeb.
17	Bitte warten
18	Maschine ausser Betrieb

The following table lists full screen messages in German:

ID	Message Text
1	Karte für internationale Auszahlungen nicht gültig.
2	Bitte Geheimzahl eingeben bei fehlerhafter Eingabe. Bitte gelbe Taste drücken.
3	Geheimzahl falsch. Bitte wiederholen.

ID	Message Text
4	Bitte betrag wählen. Maximal 20,000 ptas 2,000 5,000 10,000 15,000 20,000 ANDERE BETRAGE.
5A	Betrag in 1,000-ptas-Noten. Betrag eingeben und mit grüner Taste bestätigen. Falsche Eingabe gelbe Taste drücken.
5B	Das Gerät kann den gewünschten Betrag nicht in einem Vorgang ausgeben. Bitte wählen Sie einen kleineren Betrag.
5C	Bitte kleineren Betrag eingeben. Der höchste Betrag ist xxx,xxx ptas.
5D	Zur Zeit nur 1,000- und 5,000-ptas-Noten. Bitte Betragswahl entsprechend dieser Stückelung.
5E	Zur Zeit nur 5,000-ptas-Noten verfügbar. Bitte wählen Sie einen durch 5,000 teilbaren Betrag.
5F	Zur Zeit keine Auszahlung möglich. Bitte gehen Sie zum nächsten la Caixa-Automaten.
5G	Falsche Eingabe. Bitte wiederholen.
6	Bitte Quittung und Geld entgegennehmen.
7	Bitte Karte entnehmen.
8	Mehr als drei Fehleingaben. Der Geheimzahl Karte für Auszahlung ungültig. Bitte Karte entnehmen. Bitte sprechen Sie bei Ihrer Bank vor.
9A	Bitte Daten schneller eingeben.
9B	Vorgang abgebrochen. Bitte Quittung und Karte entnehmen.
10	Ihre Karte ist für Abhebungen an <ATM-network>-Automaten nicht geeignet.
11A	Karte verfallen. Sprechen Sie bei Ihrer Bank vor.
11B	Karte noch nicht gültig.
12	Wir wurden beauftragt Ihre Karte einzuziehen. Bitte sprechen Sie mit Ihrer Bank.
13	Vorgang abgebrochen. Bitte Quittung entgegennehmen.
14A	Maschinenfehler. Vorgang abgebrochen. Bitte Karte entnehmen.

ID	Message Text
14B	Maschinenfehler. Vorgang abgebrochen. Bitte Quittung und Karte entnehmen.
15	Karte einbehalten. Bitte während der Geschäftszeit in dieser Geschäfsstelle vorsprechen.
16	Wir wurden beauftragt Ihre Karte zurückzugeben.Bitte sprechen Sie mit Ihrer Bank
17	Bitte warten
18A	Zur Zeit keine Auszahlung. Bitte gehen Sie zum nächsten <ATM-network>-Automaten
18B	Maschine ausser Betrieb. Bitte gehen Sie zum nächsten <ATM-network>-automaten.
18C	Automat zur Zeit leider nicht betriebsbereit

D.9.2.5 Messages in Italian

The following table lists single line screen messages in Italian:

ID	Message Text
1	Carta non valida all'estero
2	Prego digitare il codice personale
3	Codice personale errato. Prego ripetere
4	Importo massimo XXXXXX CCC
5	Importo XXXXXX, cambiare se necessario
6	Prego ritirare le banconote
7	Prego ritirare la carta
8	Troppe digitazioni nel codice personale
9	Operazione annullata. Svolta lentamente
10	Carta difettosa. Prego ritirarla
11	Carta scaduta. Prego ritirarla
12	Carta trattenuta per motivi di sicurezza
13	Carta trattenuta. Operazione lenta
14	Distributore inattivo. Ritirare la carta
15	Distributore inattivo, carta trattenuta
16	Carta restituita per motivi di sicurezza

ID	Message Text
17	Attendere prego
18	Distributore automatico non in funzione

The following table lists full screen messages in Italian:

ID	Message Text
1	Carta non valida per prelievi internazionali
2	Digitare il codice personale. In caso di errore, premere il tasto giallo
3	Codice personale non corretto. Prego ripetere l'operazione
4	Indicare la somma richiesta Importo massimo 20,000 ptas 2,000 5,000 10,000 15,000 20,000 ALTRI IMPORTI
5A	Questo distributore automatico fornisce solo banconote in multipli di 1,000 ptas. Prego indicare l'importo richiesto e poi premer il tasto verde per conferma. In caso di errore, premere il tasto giallo
5B	L'importo richiesto non può essere distribuito in una sola operazione. Prego richiedere un importo minore
5C	Prego richiedere un importo minore. L'importo massimo di ciascun prelievo è di xxx,xxx ptas
5D	Sono disponibili unicamente banconote da 1,000 e 5,000 ptas. Prego indicare un importo esatto
5E	Sono disponibili unicamente banconote da 5,000 ptas.Prego indicare un importo esatto
5F	Banconote esaurite. Consultare la lista indicante il distributore automatico più vicino
5G	Operazione non corretta. Ripetere prego
6	Operazione eseguita. Prego ritirare la ricevuta e l'importo richiesto
7	Prego ritirare la carta
8	Troppe digitazioni non corrette nel codice personale. Carta non più utilizzabile nei distributori automatici. Prego ritirare la carta. Rivolgersi alla vostra banca per sostituirla
9A	Prego effettuare l'operazione più rapidamente

ID	Message Text
9B	Operazione annullata. Prego ritirare la carta e la ricevuta
10	Carta non valida nella rete <ATM-network>
11	Carta scaduta. Prego ritirare la carta. Richiedere alla vostra banca di sostituirla
11A	Carta non ancora valida
12	Ci è stato richiesto di trattenere la vostra carta. Per informazioni contattare la vostra banca
13	Operazione annullata. Prego ritirare la ricevuta
14A	Distributore automatico non in funzione. Operazione annullata. Prego ritirare la carta
14B	Distributore automatico non in funzione. Operazione annullata. Prego ritirare la carta e la ricevuta
15	Carta trattenuta per errore. Prego rivolgersi a questa agenzia durante l'orario di apertura al pubblico
16	Ci è stato richiesto di restituirvi la carta. Per informazioni consultare la lista indicante il distributore automatico più vicino
17	Attendere prego
18A	Il distributore automatico momentaneamente non è in funzione. Per informazioni consultare la lista indicante il distributore automatico più vicino
18B	Distributore automatico non in funzione. Per informazioni consultare la lista indicante il distributore automatico più vicino
18C	Servizio momentaneamente non disponibile. Ci scusiamo per ogni eventuale inconveniente

D.9.2.6 Messages in Spanish

The following table lists single line screen messages in Spanish:

ID	Message Text
1	Tarjeta sin validez internacional
2	Introduzca su número personal por favor
3	N.º personal erróneo, intente de nuevo
4	Introduzca la cantidad, máximo XXXXXX CCC
5	Cantidad XXXXXX, modifiquela si quiere
6	Por favor, retire su dinero

ID	Message Text
7	Por favor, retire su tarjeta
8	Demasiadas entradas del número personal
9	Transacción cancelada, exceso de tiempo
10	Tarjeta defectuosa. Por favor, retírela
11	Tarjeta caducada. Por favor, retírela
12	Tarjeta retenida por seguridad
13	Tarjeta retenida por limite de tiempo
14	Error en el cajero. Retire su tarjeta
15	Error en el cajero. Tarjeta retenida
16	Tarjeta devuelta por seguridad
17	Espere un momento, por favor
18	Cajero fuera de servicio

The following table lists full screen messages in Spanish:

ID	Message Text
1	Su tarjeta no es válida para operaciones internacionales
2	Introduzca su número personal
3	Número personal equivocado. Inténtelo otra vez por favor
4	Introduzca la cantidad Máximo 20,000 ptas 2,000 5,000 10,000 15,000 20,000 OTRAS CANTIDADES
5A	Este cajero solo proporciona cantidades multiplos de 1,000. Por favor, introduzca la cantidad y pulse la tecla verde. Si se equivoca, pulse la tecla amarilla.
5B	No podemos darle la cantidad solicitada. Por favor, solicite otra cantidad.
5C	Por favor, solicite una cantidad menor. El máximo permitido es xxx,xxx ptas
5D	En este momento, solo disponemos de billetes de 1,000 y 5,000 ptas. Por favor, solicite otra cantidad

ID	Message Text
5E	En este momento, solo disponemos de billetes de 5,000 ptas. Por favor, solicite otra cantidad
5F	El cajero no dispone en este momento de efectivo. Por favor, diríjase al cajero mas proximo
5G	Entrada incorrecta. Inténtelo otra vez por favor
6	Retire el recibo y su dinero por favor
7	Retire su tarjeta por favor
8	Demasiados intentos erróneos con su numero personal. Su tarjeta queda anulada. Por favor, retírela y acuda a su banco
9A	Introduzca la información mas rápido, por favor
9B	Transaccion cancelada. Retire el recibo y la tarjeta, por favor
10	Su tarjeta no es válida para los cajeros de <ATM-network>
11	Su tarjeta está caducada. Por favor, retírela y acuda a su banco
11A	Su tarjeta no es válida todavía
12	Tarjeta retenida. Por favor, acuda a su banco para mas información
13	Transaccion cancelada. Por favor, retire el recibo.
14A	Cajero fuera de servicio, transacción cancelada. Por favor, retire su tarjeta
14B	Cajero fuera de servicio, transacción cancelada. Retire el recibo y la tarjeta, por favor
15	Tarjeta retenida. Acuda a esta oficina bancaria durante las horas de oficina
16	Nos han ordenado devolverle la tarjeta. Por favor, acuda a su banco para mas información
17	Espere un momento, por favor
18A	Cajero fuera de servicio temporalmente. Por favor, diríjase al cajero mas proximo
18B	El cajero está fuera de servicio. Por favor, diríjase al cajero mas proximo
18C	Servicio no disponible en este momento. Disculpe las molestias

Appendix E Glossary

Glossary

This section defines various terms, concepts, acronyms, and abbreviations used in this document. These definitions appear for convenience only and are not to be used or otherwise relied on for any legal or technical purpose. MasterCard specifically reserves the right to amend any definition appearing herein and to interpret and apply all such definitions in its sole discretion as MasterCard deems fit.

AAC

See application authentication cryptogram.

AC

See application cryptogram.

adjustment

An entry initiated by an Acquirer to correct a system error or an inaccurate record of a Transaction, and affecting the movement of funds between the Issuer and Acquirer with respect to such Transaction.

advice

A message that notifies a party of an action that has been taken, requiring no response.

ANSI

American National Standards Institute.

application authentication cryptogram (AAC)

An application cryptogram generated by a Chip Card when declining a Transaction.

application cryptogram (AC)

A cryptogram generated by the Chip Card in response to a GENERATE AC command. The three types of cryptograms are TC, ARQC, and AAC.

application identifier (AID)

A numbering system and registering procedure for identifying specific companies and their chip-based products, as defined by ISO/IEC 7816-5. The application identifier has two components: the Registered Application Provider Identifier (RID) and the Proprietary Application Identifier Extension (PIX).

application label

Mnemonic associated with the AID according to ISO/IEC 7816-5. This field, which is up to 16 characters long, allows for global interoperability. The application preferred name, if available, overrides the application label.

application preferred name

Preferred mnemonic associated with the AID, as specified by the Issuer. This field is up to 16 characters long. The application preferred name, if available, overrides the application label.

approval code

The code given online by the Issuer (or its agent) to the card when an authorization request has been approved. This code acts as proof of authorization.

ARQC

See authorization request cryptogram.

authorization

Approval of a transaction by or on behalf of an Issuer in accordance with the Standards. The merchant receives, via telephone or authorization terminal, this approval to process the transaction.

authorization request cryptogram (ARQC)

An application cryptogram generated by a Chip Card when requesting online authorization.

Automated Clearing House (ACH)

A group of processing institutions networked together to exchange and settle electronic debit transactions.

balance inquiry

A non-financial Transaction initiated by the Cardholder in which the Cardholder's balance is displayed and/or printed. Use of a PIN is required.

balance response

Automatic communication by the Issuer of the remaining balance on a prepaid Card within the authorization response on a financial Transaction. Also referred to as referred to as account balance response.

bank identification number (BIN)

A unique number that appears as the first digits in the PAN and is assigned to identify a group of cards belonging to an Issuer for the purposes of routing. (See IIN.)

block/unblock

The Issuer-initiated suspension (blocking) and re-activation (unblocking) of the live application on a Chip Card. An Issuer can block the live application on a Chip Card during any online dialogue or transaction using script processing.

business day

A "Business Day" as defined in Regulation CC of the Board of Governors of the U.S. Federal Reserve System, 12 C.F.R. Pt. 229.

cancel

A Transaction initiated by the cardholder and/or Merchant to notify the Issuer by means of an online reversal that the Transaction authorization should be reversed. This Transaction may be initiated either before or after an authorization response is received by the Acquirer.

Card acceptance or acceptor device (CAD)

A hardware device (such as an ATM) used to capture and transmit payment card and that may be connected to a remote computer system; such as an Acquirer network, or may operate as a stand-alone device.

Card authentication method (CAM)

A procedure which takes place between a Card and the Terminal and/or Issuer to verify that the Card is genuine.

cardholder-activated terminals (CAT)

A cardholder-activated, chip or magnetic stripe-reading POS Terminal, (usually unattended) that dispenses a product or provides a service when activated by a Cardholder.

card-to-card authentication (CCA)

Card authentication as a result of interaction between two active Chip Cards: the Cardholder's Card and the Merchant's chip (which may be embedded in a removable Card or may be a permanent part of the POS Terminal), interacting via a passive terminal, without online contact to the Issuer. Both chips issue challenges to each other and verify the result.

Cardholder verification method (CVM)

A system or technology used to verify that the person presenting a Card is the authorized Cardholder.

Card-read

A Transaction authorized and settled electronically where full magnetic stripe or chip data is read by a Terminal and transmitted in its entirety to the Issuer.

checking account (DDA)

A demand deposit, negotiable order of withdrawal, share draft, or other transaction account which normally requires an Issuer to pay immediately upon proper presentation of a negotiable order to pay.

chip

A piece of silicon etched with electronic circuits. A microprocessor chip has an operating, a programming, and a data memory that allows internal processing to take place and provides additional storage capacity.

clearing

The process of exchanging Transaction details between an Acquirer and an Issuer to facilitate both the posting of Transactions to the Cardholder's Account and the reconciliation of a Customer's settlement position.

co-branded card program

A program aimed at issuing Cards to the customer base of a retailer, service provider or other commercial organization.

communication key

A cryptographic key used for the encipherment and decipherment of cryptographic keys. Also called a "key enciphering key."

compliance

The procedure used to resolve disputes between two Customers involving an alleged violation of the Rules for which no chargeback reason applies.

correction

A credit intended to correct an error in connection with a prior Transaction that covers all or part of the amount of such prior Transaction.

credit card

A plastic card bearing an account number assigned to a Cardholder with a credit limit that can be used to purchase goods and services and to obtain cash disbursements on credit, for which a Cardholder is subsequently billed by an Issuer for repayment of the credit extended at once or on an installment basis.

credit card account

A transaction account held by an Issuer that represents a revolving line of credit or pre-approved loan from which funds may be extended upon proper presentation of a request to pay.

cryptogram

The output from the process of transforming cleartext into ciphertext for security or privacy.

data encryption standard (DES)

A cryptographic algorithm adopted by the U.S. National Bureau of Standards for data security. Encryption scrambles PINs and transaction data for safe transmission.

debit card

A plastic card used to initiate a debit Transaction. In general, these Transactions are used primarily to purchase goods and services and to obtain cash, for which the Cardholder's asset Account is debited by the Issuer.

Debit MasterCard card

A card bearing the MasterCard mark issued by a MasterCard International customer or affiliate which provides access to a cardholder deposit account for making purchases or withdrawing cash.

decline

Authorization response whereby the Issuer (or its agent) has refused to authorize the Transaction.

digital wallet

See remote wallet.

downtime

The period during which computer or network resources are unavailable to users because of a failure or normal downtime maintenance.

dual currency environment

A country, territory or zone in which two (2) currencies with different denominations coexist as legal currency.

dynamic data authentication (DDA)

An offline Card authentication technique in which the Chip Card and the Terminal must be active and capable of executing a public key algorithm. This process produces a unique digital signature for each authentication attempt thereby eliminating the possibility of replay.

dynamic stand-in authorization

Where allowed by a Region, authorization given by the Interchange System on behalf of the Issuer and at the Issuer's risk, according to a number of risk parameters specified by the Issuer. It is activated dynamically, for example if the Issuer is unavailable due to network failure or if the authorization response comes too late or not at all.

electronic commerce Transaction

A non face-to-face online Transaction that uses electronic media over a public network (such as the Internet) or private network (such as an extranet).

electronic funds transfer (EFT)

A paperless transfer of funds initiated from a POI Terminal, computer, telephone instrument, or magnetic tape.

emergency BIN list

An exceptions file that is resident either in the POS Terminal or Terminal or the Acquirer host. It contains Card BINs or BIN ranges. It is intended for use in an emergency situation where Maestro needs to restrict the use of a large number of compromised Cards or in case of Customer failure.

EMV (Europay-MasterCard-Visa)

A set of technical specifications agreed between MasterCard, MasterCard Europe, and Visa designed to ensure global chip bankcard interoperability.

encryption keys

A component of the security algorithms used to protect data.

European Economic Area (EEA)

The following countries comprise the European Economic Area (EEA): 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.

fallback

Customers use fallback procedures when a Chip Card is present at a hybrid POS Terminal or Terminal and the Acquirer processes the Transaction by using the magnetic stripe because the Acquirer cannot process the Transaction using chip technology.

Financial Institution Table (FIT)

The computer resident table of Customers' Card prefixes or BINs/IIN used for Transaction routing.

GCMS

See Global Clearing Management System.

global bank

A financial institution which is a majority owner of financial institutions in more than one (1) country.

global bank holding company

A bank holding company, which is a majority owner of financial institutions in more than one (1) country.

Global Clearing Management System (GCMS)

A centralized clearing facility owned and operated by MasterCard for the daily processing and routing of worldwide financial transactions between MasterCard and its Customers.

institution definition file (IDF)

The computer-resident table used to identify Customers in the Corporation.

institution identification number (IIN)

A unique number that appears as the first digits in the PAN and is assigned to identify a group of cards belonging to an Issuer for the purposes of routing. (*See* BIN).

institution routing table (IRT)

The computer-resident table of Issuers' Card prefixes or BINs/IINs used for Transaction routing.

interchange fee

A fee applied to an interchange Transaction, applicable to the two Customers participating in the Transaction as Issuer and Acquirer.

International Organization for Standardization (ISO)

An international body that provides standards for financial transactions and telecommunication messages. ISO works in conjunction with the Consultative Committee for International Telephone and Telegraph (CCITT) for standards that impact telecommunications. ISO supports specific technical committees and work groups to promulgate and maintain financial services industry standards, such as BINs/IINs and merchant category codes.

Internet Protocol-enabled terminal

Any POS terminal that uses Web-based communication protocols.

interregional

Activities or events involving multiple Regions.

intraregional

Activities or events involving a single Region.

Integrated Product Message (IPM)

A format for processing of clearing activity and interchange-related activity. The message format uses a variable-length and variable-format structure based on the ISO 8583-1993 standard.

ISO 9564

The ISO document entitled Banking – Personal Identification Number Management and Security. It is comprised of Part I – Basic Principles, and Requirements for Online PIN Handling in ATM and POS Systems and Part II – Approved Algorithm(s) for PIN Encipherment.

key

A sequence of symbols that control the operation of a cryptographic transformation.

magnetic stripe

The magnetically encoded stripe on the bankcard plastic that contains information pertinent to the Cardholder Account. The physical and magnetic characteristics of the magnetic stripe are specified in ISO Standards 7810, 7811, and 7813.

master key

A cryptographic key used to encipher and decipher communication keys.

merchant category code (MCC)

A four-digit classification code used in authorization, clearing, and other transactions or reports to identify the type of merchant.

Merchant discount fee

The fee the Merchant pays to its Acquirer to acquire Transactions.

network

The Interchange System and the Regions together with all other computer hardware and software, telecommunications facilities and equipment, the Service Marks, Rules, the technical specifications, and all agreements used by Maestro, for the purpose of supporting interchange.

network zone

The logical transmission path between two INFs.

offline

An operating mode for a Transaction or a specific message component of a Transaction (such as a request to verify the Cardholder [CVM], to authenticate the Card [CAM] or to authorize the amount of the Transaction) in which the POS Terminal does not communicate with the central computer system operated by the Issuer (or its agent). In this mode, the responses to certain instructions generated by the POS Terminal necessary to approve or decline the Transaction are governed by the parameters or guidelines set within the POS Terminal and the Chip Card.

offline PIN or offline PIN verification

A technology used to initiate a Transaction with a Chip Card in which the cardholder verification method (CVM) is a PIN to be verified offline at the hybrid POS Terminal against a reference PIN stored in the Chip Card.

offline Transaction

A Transaction that is processed without contacting the Issuer (or its agent).

online

An operating mode for a Transaction or a specific message component of a Transaction (such as a request to verify the Cardholder [CVM], to authenticate the Card [CAM] or to authorize the amount of the Transaction) in which the Terminal or the POS Terminal is required to communicate with the central computer system operated by the Issuer (or its agent). In this mode, the responses to certain instructions generated by the Terminal or the POS Terminal necessary to approve or decline the Transaction are governed by the parameters or guidelines set within the Issuer's database and accessed by such central computer system.

online mutual authentication (OMA)

A process by which a Chip Card and its Issuer authenticate each other, which can occur only when an online authorization request to the Issuer is initiated. The process may be based on the Issuer's secret keys stored on the chip.

online PIN or online PIN verification

A technology used to initiate a Transaction with a Chip Card or a magnetic stripe card in which the cardholder verification method (CVM) is a PIN sent online by the ATM to be verified against a PIN stored in the Issuer's database.

online Transaction

A Transaction that is processed where there is real-time dialogue between the Acquirer and the Issuer (or its agent).

OMA

See online mutual authentication.

partial reversal

A reversal in which the original Transaction was approved for a greater amount than was completed by the Acquirer, and the difference between the amount of such original Transaction and the amount that was completed is reversed.

pass-through account

"Pass-through account" means an account for which the funds ultimately come from another account, which is maintained by an entity other than the institution that maintains the pass-through account. Pass-through accounts are also commonly known as "sweep accounts" or "zero-balance accounts."

payment gateway

The Acquirer system that receives messages via open systems from the merchants, performs certain functions and acts as the bridge to the closed systems used for normal card payment transactions.

payment system

System that accomplishes the transfer of money.

personal identification number (PIN)

The unique, confidential number assigned to, or selected by, a cardholder to provide legal identification when used in an electronic funds transfer environment.

physically secure device

A type of tamper-resistant security module that protects any cryptographic key or PIN resident within the device against penetration attacks. Penetration of a physically secure device will cause the automatic and immediate erasure of all PINs, cryptographic keys, and all useful residue of PINs and keys contained within the device. A device is considered to be a physically secure device only when the device's internal operation cannot be and has not been modified to allow penetration. Also called a tamper-responsive device. See tamper-resistant security module (TRSM).

PIN-based Transaction (PBT)

A Transaction verified by the use of a Cardholder's PIN.

PIN block

The PIN and other information necessary to de-encrypt, re-encrypt, or verify PIN information.

PIN entry device

A keyboard device attached to an electronic payment terminal that enables the Cardholder to enter a PIN.

PIN verification

A procedure that enables the Issuer to validate the Cardholder identity when making a comparison with the PIN and Cardholder Account number.

pre-authorization

A pre-authorization is a non-posting authorization Transaction that will subsequently be followed by a separate financial Transaction within a specific time interval. The subsequent financial Transaction will be a posting Transaction against the Cardholder's Account. Pre-authorizations are used primarily in POI situations where the Cardholder wishes to obtain "advance approval" or "verification" that sufficient funds are available to make a subsequent purchase using a debit card.

pre-authorization completion

A transaction used by the Acquirer to notify the Issuer of the final outcome of a previously approved pre-authorization. A pre-authorization completion must be sent for any approved pre-authorization.

prefix number

When used together, the major industry identifier and the IIN are known as a prefix number.

primary account number (PAN)

The number that is embossed, encoded, or both, on a Card that identifies the Issuer and the particular Account. The PAN consists of a major industry identifier, BIN/IIN, individual account identifier, and check digit.

primary application

The payment application supported by a hybrid Card that corresponds to the visible branding on the Card. Only one primary application may reside on a Card.

proprietary card

A type of card that financial institutions or other organizations issue using the logo of the Issuer instead of a national service mark or logo (such as MasterCard). A proprietary card allows the cardholder to access a credit or deposit account using ATM or POI terminals.

proprietary transaction

Any transaction initiated with a Card or a card at a Terminal or any terminal owned or operated by or for the Customer that issued that Card or card, or by or for an Affiliate of the Customer within the same bank holding company.

purchase

A financial transaction, if approved, in which funds are debited by the Issuer from the Cardholder's Account and credited to an Acquirer for the payment of goods or services by the Cardholder to a Merchant of such Acquirer.

receipt

A hard copy document recording a Transaction that took place at the Point of Interaction, with a description that usually includes: date, Merchant name/location, primary account number, amount, and reference number.

refund

A Transaction where the Cardholder returns goods to the Merchant and is credited for the value. A full or partial refund of the initial Transaction is possible. The Cardholder authorization payment fee relative to the Amount refunded is reversed. Since this is a separate Transaction from the original purchase, the foreign exchange rate applied, if applicable, may vary from that applied to the original Transaction.

related data

Data required by the Issuer to validate a transaction certificate. Related data appears in data element 55.

required data

The minimum data required to be stored on a chip to perform a Transaction. (For example: PAN, expiration date and service code.)

response code

A code used to indicate the status of a Transaction or message or to indicate an action taken or that is required.

resubmission

The electronic submission of a Transaction that was initially stored by the Acquirer or Merchant pursuant to the provisions governing Merchant-approved Transactions.

reversal

A message informing the receiver that the sender has canceled a previous record.

savings account

A time deposit transaction account that normally does not require an Issuer to pay immediately upon proper presentation of an order to pay.

scrip

A printed receipt which must be exchanged at a designated location for goods or services.

script processing

The process by which the Issuer can send a set of commands to the Card. For example: for purposes of PIN unblocking or parameter modifications.

security module

A physically secure device possessing specialized security features and functions required for cryptographic PIN security and dynamic key management.

service code

Part of the data of the magnetic stripe, which signifies the extent of interchange/technology permitted, the authorization processing allowed for the Card by the Issuer, and the range of services available on the Card, including the details of PIN requirements imposed by the Issuer.

settlement account

An account that each Customer must maintain for the purpose of settlement.

signature-based transaction (SBT)

A Transaction for which the CVM is signature.

smart card ATM technology

A Chip Card located in an ATM that conforms to the standards set forth in *Tamper Resistance—A Smart Card Integrated Circuit Security Guideline*, and provides hardware-based cryptographic ATM functions.

static data authentication (SDA)

Authentication of a Chip Card as a result of interaction between a hybrid POS Terminal or Terminal and the Chip Card, without online authentication to the Issuer. The POS Terminal or Terminal verifies the Card's fixed cryptographic signature. During SDA, the Card is passive and the POS Terminal or Terminal is active.

store and forward (SAF)

A process by which Transaction messages that could not be immediately delivered, (for example, due to communication problems and so on), are automatically saved for future delivery, and then transmitted at some later time to the intended receiver.

system to avoid fraud effectively (SAFE)

A central repository for fraud data from which monthly reports and statistics are derived and sent to Customers. SAFE assists Customers in the detection and prevention of fraud in addition to providing Customer fraud data.

surcharge

Any fee charged to the Cardholder in connection with a Transaction that is not charged if another payment method is used.

tamper evident characteristics

Cryptographic device characteristics as published in ISO 13491-1, Banking—Secure Cryptographic Devices—part 1 Concepts, Requirements and Evaluation Methods.

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. *See* tamper-resistant security module (TRSM).

tamper resistance

The physical capability of components within a system to withstand external attack and, if necessary, to destroy any confidential information contained therein.

tamper-resistant security module (TRSM)

A hardware device that meets the requirements of a physically secure device as defined in ISO 9564-1. The TRSM is used to ensure that the cardholder PIN and the PIN keys used to encrypt and decrypt the PINs are protected against external attacks. See physically secure device, tamper-evident device.

tamper-responsive device

See physically secure device.

TC

See transaction certificate.

technical fallback

A Transaction in which a Hybrid POS Terminal or Terminal processes a Chip Card using magnetic stripe technology because the Transaction could not be completed using chip technology.

terminal response time

The time required to receive an approval or denial response to a Transaction request, after entry of the Transaction and the Cardholder PIN, where required, at the Point of Interaction.

track 1

The first magnetic track on a Card. It is read-only, and its contents are defined in ISO 7813.

track 2

The second magnetic track on a Card. It is read-only, and its contents are defined in ISO 7813.

Transaction certificate (TC)

An application cryptogram generated by a Chip Card when accepting a Transaction.

Transaction date

The date a Cardholder effects a Card purchase of goods, services, or other things of value, or effects a cash disbursement.

Transaction response

An electronic message sent to the Acquirer, by the Issuer, in response to a Transaction request.

Transaction time

The local time at which the Transaction was initiated at a POS Terminal or Terminal.

type-approval

A process set by MasterCard to ensure compliance with the chip specifications as published by MasterCard and EMVCo from time to time.

universal cardholder authentication field (UCAF)

A field to support a universal multipurpose data transport infrastructure that the Corporation uses to communicate authentication information among the Cardholder, Merchant, Issuer, and Acquirer communities.

working key

A cryptographic key used to encipher and decipher PINs (sometimes referred to as PIN encipherment).

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access is a specification of security enhancements to the IEEE 802.11b (Institute of Electrical and Electronics Engineers Inc.) specifications derived from the IEEE 80211i draft. It was designed to address security vulnerabilities found in the Wireless Equivalent Privacy protocol (WEP) and will be forward compatible with the 80211i standard when it is finalized.

Wireless Local Area Network (LAN)

A wireless network that uses radio waves, microwaves, or both to communicate and transmit data between and among computers and devices equipped with wireless capability. Wired networks, on the other hand, use physical cable connections. Wireless LAN refers to the 802.11 family if specification developed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE). These standards specify an over-the-air interface between a wireless client and a base station, or between two wireless clients. It includes standards such as 802.11b (more popularly known as Wi-Fi) as well as 802.11a and 802.11g which specify the behavior of wireless networks operating at varying frequencies.