



# *PayPass* M/Chip Acquirer Implementation Requirements

Version 1.0 - July 2008

## **Proprietary Rights**

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

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

## **Trademarks**

Trademark notices and symbols used in this manual 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.

## **Media**

This document is available on [www.paypass.com](http://www.paypass.com).

MasterCard Worldwide - CCOE  
Chaussée de Tervuren, 198A  
B-1410 Waterloo

Belgium

[www.mastercard.com](http://www.mastercard.com)

## Using this Document

Purpose.....	1
Scope .....	1
Audience.....	2
Overview .....	2
Excerpted Text .....	3
Language Use .....	3
Terminology .....	3
Related Publications .....	4
Product Independent Documentation.....	4
MasterCard Specific Documentation.....	5
Maestro Specific Documentation.....	6
Related Information.....	6
Abbreviations.....	7
Further Information .....	8

## Chapter 1 Introduction

1.1 Product Overview .....	1-1
1.2 Interoperability .....	1-1
1.2.1 MasterCard <i>PayPass</i> .....	1-1
1.2.2 Maestro <i>PayPass</i> .....	1-1
1.3 Implementation and Prerequisites Summary .....	1-1
1.4 Transaction Flow Enhancements for <i>PayPass</i> .....	1-2

## Chapter 2 Acquirer and Merchant Requirements

2.1 Overview .....	2-1
2.1.1 Program Enrollment .....	2-1
2.1.2 Terminal Selection.....	2-1
2.1.3 Branding .....	2-2
2.1.4 <i>PayPass</i> Readers .....	2-2
2.1.5 Terminal/Reader Environment.....	2-3
2.1.6 Terminal Application – Technical Requirements .....	2-3
2.2 Supporting Other Payment Acceptance Methods at <i>PayPass—M/Chip</i> Terminals.....	2-4
2.2.1 Accepting <i>PayPass—Mag</i> Stripe and Cardholder Devices (non card form factors) .....	2-4
2.2.1.1 MasterCard <i>PayPass</i> .....	2-4
2.3 New Limits used for <i>PayPass—M/Chip</i> .....	2-6
2.3.1 New Contactless Limit Data Items .....	2-6
2.3.1.1 Terminal Contactless Transaction Limit .....	2-6
2.3.1.2 Terminal CVM Required Limit .....	2-6
2.3.1.3 Terminal Contactless Floor Limit.....	2-8
2.3.2 Hard and Soft Limit Implementations .....	2-8
2.4 <i>Transaction</i> Processing.....	2-9
2.4.1 <i>PayPass—M/Chip</i> Transaction Types.....	2-9
2.4.1.1 Reversals.....	2-9
2.4.1.2 Cancellations .....	2-9
2.4.1.3 Refunds.....	2-9
2.4.2 Application Selection and Cardholder Confirmation .....	2-10
2.4.3 Amount Entry at Attended POS .....	2-10
2.4.3.1 Gratuities/‘Tips’ .....	2-10
2.4.4 Cardholder Verification .....	2-10
2.4.4.1 MasterCard <i>PayPass</i> Cardholder Verification.....	2-10
2.4.4.2 Maestro <i>PayPass</i> Cardholder Verification .....	2-11
2.4.4.3 Offline PIN .....	2-11
2.4.5 Offline Data Authentication Requirements .....	2-11
2.4.6 Service Code Checking.....	2-12
2.4.7 Terminal Risk Management .....	2-12
2.4.7.1 Floor Limit Check – Cumulative Transaction Amount Checking.....	2-12
2.4.7.2 Random Transaction Selection .....	2-13
2.4.7.3 Velocity Checking.....	2-13
2.4.7.4 Exception File Checking.....	2-13

2.4.8 Online/Offline Terminal Requirements.....	2-13
2.4.9 Clearing.....	2-13
2.4.10 Declined Transactions and Issuer Responses.....	2-14
2.4.10.1 Pick-up/Capture Card Responses.....	2-14
2.4.10.2 Online Declines.....	2-14
2.4.10.3 Card Declines.....	2-14
2.4.10.4 “Referrals”/”Call Me” Issuer Responses.....	2-14
2.5 Receipt Printing.....	2-15
2.6 Fallback for PayPass Transactions.....	2-16
2.7 Terminal and Network Performance.....	2-17

## Chapter 3 Terminal Configuration Data

3.1 <i>PayPass—M/Chip</i> Specific Terminal Data.....	3-1
3.2 AIDs and Related Application Labels.....	3-2
3.3 Application Version Number.....	3-4
3.4 <i>PayPass</i> Limits.....	3-4
3.4.1 Maestro <i>PayPass</i> Limits.....	3-4
3.4.2 MasterCard <i>PayPass—M/Chip</i> Limits.....	3-4
3.4.2.1 Terminal Contactless Transaction Limit.....	3-5
3.4.2.2 Terminal CVM Required Limit.....	3-5
3.4.2.3 Terminal Contactless Floor Limit.....	3-5
3.5 Terminal Action Codes (TACs).....	3-6
3.5.1 Terminal Action Codes - Online Capable Terminals.....	3-7
3.5.2 Terminal Action Codes - Offline Only Terminals (CAT3).....	3-9
3.6 Terminal Capabilities.....	3-11
3.7 Terminal Type.....	3-12

## Chapter 4 Network Interfaces and Host Systems

4.1 Summary of Changes .....	4-1
4.2 Authorization Requests .....	4-2
4.3 Authorization Responses.....	4-4
4.4 Clearing.....	4-4
4.5 Chargebacks .....	4-6
4.5.1 MasterCard Chargebacks.....	4-6
4.5.2 Maestro Chargebacks .....	4-7

## Chapter 5 Testing

5.1 Testing Overview .....	5-1
5.2 Testing Scope by PayPass Terminal Type.....	5-1
5.3 Testing Process.....	5-1
5.4 Test Stages .....	5-2
5.5 NIV.....	5-3
5.5.1 Offline Authorization Testing (Mandatory) .....	5-3
5.5.2 Conditional Offline Clearing Testing .....	5-3
5.5.3 Optional Online Testing .....	5-3
5.6 TIP.....	5-4
5.7 ETED.....	5-5
5.8 Post-Live Monitoring .....	5-5
5.9 Further Information and Contact Details.....	5-6

**Appendix A PayPass—M/Chip Limit Use – Functional Implementation Examples**

A.1 Soft Limit Implementations..... A-1

A.2 Hard Limit Implementations..... A-4

**Appendix B Glossary**

Glossary of Terms ..... B-1



---

## Using this Document

*This chapter contains information that helps you understand and use this document.*

---

Purpose .....	1
Scope .....	1
Audience .....	2
Overview .....	2
Excerpted Text .....	3
Language Use .....	3
Terminology .....	3
Related Publications .....	4
Product Independent Documentation.....	4
MasterCard Specific Documentation .....	5
Maestro Specific Documentation.....	6
Related Information.....	6
Abbreviations.....	7
Further Information.....	8



## Purpose

The MasterCard *PayPass M/Chip Implementation Requirements* defines requirements for acquirers implementing the MasterCard *PayPass—M/Chip* program.

These implementation requirements assume an implementation on top of an acquirer's existing EMV (contact) deployment.

For further information on migrating to contact EMV refer to the *M/Chip Customer Implementation Guide*.

## Scope

This document defines implementation requirements for *PayPass—M/Chip* acquiring based on MasterCard technical and business requirements. It provides a level of detail that will enable acquirers to identify the required system changes. This includes information on terminal functionality and configuration. Further detailed information on the *PayPass* and *M/Chip* technology is available in the corresponding specification documents. The reader may need to refer to these for a deeper understanding of the technology or areas outside the scope of an acquirer implementation.

The requirements are for *PayPass* implementations of the MasterCard and Maestro products only. MasterCard requirements refer to both MasterCard Debit and MasterCard Credit unless specifically stated. Unless otherwise stated the document contents apply to both MasterCard and Maestro. The terms '*PayPass*' and '*PayPass—M/Chip*' are used generically unless specifically referring to a card product.

The following are outside the scope of these requirements:

- Implementing EMV acquiring. Only the additional requirements for *PayPass—M/Chip* are addressed in this document
- ATMs, bank branch terminals, Cardholder Activated Terminals levels 4–8 or transactions
- e-Commerce acquiring and transactions
- Cash advance and purchase with cashback transactions



### Note

**These requirements are focused on the acquirer acceptance of *PayPass—M/Chip* cards and make specific reference to *PayPass—Mag Stripe* where necessary.**

## Audience

This document is intended for use by acquirers and payment processors implementing *PayPass* acceptance.

It is assumed that the audience is already familiar with EMV Chip acceptance in general.

## Overview

This document is a guide for acquirers implementing *PayPass—M/Chip*. It details the requirements, impacts, and any necessary implementation data or configurations.

*PayPass—M/Chip* implementations are an extension to an acquirer EMV Chip implementation.

The following table provides an overview of the chapters in this manual:

CHAPTER	DESCRIPTION
Using this Document	This chapter contains information that helps you understand and use this document.
Chapter 1: Introduction	This chapter provides introduction and overview of implementing <i>PayPass—M/Chip</i> acceptance.
Chapter 2: Acquirer and Merchant Terminal Requirements	This chapter explains the MasterCard requirements for implementing <i>PayPass—M/Chip</i> acceptance.
Chapter 3: Terminal Configuration Data	This chapter provides further information on how to configure <i>PayPass—M/Chip</i> specific data based on the requirements in Chapter 2.
Chapter 4: Network Interfaces and Host Systems	This chapter summarizes the impacts and changes to network and host system interfaces.
Chapter 5: Testing	This chapter provides an overview of the testing process required for <i>PayPass—M/Chip</i> implementation.
Appendix A: <i>PayPass—M/Chip</i> Limit Use – Functional Implementations	This appendix illustrates valid implementations of the <i>PayPass—M/Chip</i> Limits.
Appendix B: Glossary	This appendix is a Glossary of Terms used in this document.

## Excerpted Text

At times, this document may include text excerpted from another document. A note before the repeated text always identifies the source document. In such cases, we included the repeated text solely for the reader's convenience. The original text in the source document always takes legal precedence.

## Language Use

The spelling of English words in this manual follows the convention used for U.S. English as defined in Webster's New Collegiate Dictionary. An exception to the above concerns the spelling of proper nouns. In this case, we use the local English spelling.

Requirements are documented using the following definitions:

- “Must” - indicates a mandatory requirement.
- “Should” – indicates a recommendation, or best practice.
- “May” – defines a product or system capability which is optional or a statement which is informative only.

## Terminology

The following provides some specific clarifications on terms used in this document including previous or alternative terms with the same meaning.

<b>Term</b>	<b>Clarification</b>
Cardholder Device	Previous/alternative term(s) used: Non-card form factor (NCFF)
Hard / Soft limit implementations	The configuration of <i>PayPass</i> —M/Chip limits results in one of these implementation types within a Region or Market..A market is soft limit unless agreed with MasterCard.
Terminal Contactless Floor Limit	Previous/alternative term(s) used: <i>PayPass</i> Floor Limit
Terminal Contactless Transaction Limit	Previous/alternative term(s) used: Hard Limit Contactless Transaction Limit Ceiling Limit (In Maestro <i>PayPass</i> Global Rules)

## Using this Document

### Related Publications

---

Term	Clarification
Terminal CVM Required Limit	Previous/alternative term(s) used: CVM and Receipt Limit Chargeback Protection Amount

## Related Publications

The following publications contain material directly related to the contents of this book. Interim updates and announcements are communicated in MasterCard bulletins.

### Product Independent Documentation

The following documentation is not specific to the *PayPass* product.

Document	Relevance
AS2805 Message Formats (authorizations)	Defines MasterCard AS2805 Authorization interface
Customer Interface Specification (authorizations)	Defines the MasterCard Authorization interface to BankNet
GCMS Release Document (clearing)	Defines MasterCard Global Clearing Management System (GCMS). (Messaging interfaces are described in the IPM and MDS documentation)
Global Operations Bulletin No. 6, June 2005	Summarizes the initial <i>PayPass</i> release in one document. (Changes are incorporated in all current documentation where relevant)
Chargeback Guide	Defines MasterCard global chargeback rules, including <i>PayPass</i> related chargebacks
Integrated Product Messages (IPM) Clearing Formats (clearing)	Defines the clearing interface to MasterCard GCMS using IPM formats
M/Chip Customer Implementation Guide	A guide to implementing EMV contact for MasterCard products
M/Chip Requirements	MasterCard requirements for contact EMV
M/Chip Program Guide	Explains the MasterCard M/Chip program and provides supporting information on how EMV functions work
MasterCard Debit Switch (MDS) online specifications Message Formats	Message formats for the single message interface to the MasterCard Debit Switch (Debit)

Document	Relevance
<i>PayPass</i> —M/Chip Technical Specifications* (and Application Notes) – Part II  *NOTE: Future release will be called	The principal reference document for MasterCard <i>PayPass</i> Technical Requirements
<i>PayPass</i> —M/Chip Interface and Interoperability Requirements	
<i>PayPass</i> Terminal Vendor Testing Process Manual	Describes the process for vendor testing of <i>PayPass</i> terminals
V5 Interface Specification (authorizations)	Provides details of the authorization interface to EPSNet
Terminal Implementation Process (TIP) Guide	Describes MasterCard TIP testing for EMV contact and <i>PayPass</i>
Global Network Interface Validation Document Set (GNIVD)	Provides details of the network interface validation process, the procedures to be followed, and the pre-defined test cases that may be conducted for network interface testing and validation for existing and new customers
MasterCard <i>PayPass</i> Terminal implementation Requirements	Describes the generic requirements for all <i>PayPass</i> accepting terminals
MasterCard <i>PayPass</i> Terminal Optimization Guide	Describes suggests technical optimization to achieve fast <i>PayPass</i> transactions

## MasterCard Specific Documentation

Document	Relevance
MasterCard <i>PayPass</i> Branding Standards Manual	Defines MasterCard Branding Requirements, (for example the landing zone design)
MasterCard <i>PayPass</i> Product Guide	A business guide to the MasterCard <i>PayPass</i> product

## Maestro Specific Documentation

Document	Relevance
Maestro <i>PayPass</i> Branding Standards	Defines MasterCard Branding Requirements for Maestro <i>PayPass</i>
Maestro Global Rules	Defines Maestro Global rules, including Maestro <i>PayPass</i>
Global Operations Bulletin No. 2, 1 February 2008 “Launch of Maestro <i>PayPass</i> ”.	Defines and describes the initial launch of Maestro <i>PayPass</i> .

## Related Information

The following reference materials may be of use to the reader of this manual:

Document	Details
ISO/IEC 7811/2	Identification cards—recording technique—Part 2: magnetic stripe
ISO/IEC 7813:1995	Identification cards—financial transaction cards
EMV BOOK 1	Integrated Circuit Card Specification for Payment Systems: Application Independent ICC to Terminal Interface Requirements. Version 4.1 June 2007
EMV BOOK 2	Integrated Circuit Card Specification for Payment Systems: Security & Key Management. Version 4.1 June 2007
EMV BOOK 3	Integrated Circuit Card Specification for Payment Systems: Application Specification. Version 4.1 June 2007
EMV BOOK 4	Integrated Circuit Card Specification for Payment Systems: Cardholder, Attendant and Acquirer Interface Requirements. Version 4.1 June 2007
EMV Contactless Communication Protocol Specification v2.0	This book defines the EMV Contactless Communication Protocol Specification v2.0
EMV Contactless Specifications for Payment Systems – Entry Point Specification	This book defines the EMV Contactless Specifications for Payment Systems – Entry Point Specification
EMV Contactless Specifications for Payment Systems – Framework for Contactless Evolution	This book describes the EMV Contactless Specifications for Payment Systems – Framework for Contactless Evolution

Document	Details
EMV SU44	This book describes the EMV SU44 - Specification Update Bulletin no.44, CDA Modified Terminal Behaviour

## Abbreviations

The following abbreviations are used in these requirements:

Abbreviation	Description
AC	Application Cryptogram
AID	Application Identifier
ASI	Application Status Indicator
CAM	Card Authentication Method
CAT	Cardholder Activated Terminal
CDA	Combined DDA/Application Cryptogram Data Authentication
CVC	Card Verification Code
CVM	Cardholder Verification Method
DDA	Dynamic Data Authentication
ECR	Electronic Cash Register
ETEC	Easy Test Cards
ETED	End-to-End Demonstration (testing)
EMV	Europay MasterCard Visa
Hex	Hexadecimal
ICC	Integrated Circuit Card
IIN	Issuer Identification Number
ISO	International Organization for Standardization
NIV	Network Interface Validation
NCFE	Non-Card Form Factor
PAN	Primary Account Number
PIN	Personal Identification Number
PIX	Proprietary Application Identifier Extension
POS	Point of Sale
RFU	Reserved for Future Use

## Using this Document Further Information

---

Abbreviation	Description
SDA	Static Data Authentication
TAC	Terminal Action Codes
TDOL	Transaction Certificate Data Object List
TIP	Terminal Integration Process
TRM	Terminal Risk Management

## Further Information

Further information on the above and the overall *PayPass* program is available in the MasterCard *PayPass* Product Guide and the *PayPass* Technical Specifications. Questions may also be addressed to the following e-mail addresses:

General: [paypass@mastercard.com](mailto:paypass@mastercard.com)

Specifications: [specifications@paypass.com](mailto:specifications@paypass.com)

Testing: [testing@paypass.com](mailto:testing@paypass.com)

Chip Technical Help: [chip\\_help@mastercard.com](mailto:chip_help@mastercard.com)

---

# 1

## Introduction

*This chapter provides an introduction and overview of implementing PayPass—M/Chip acceptance*

---

1.1 Product Overview .....	1-1
1.2 Interoperability .....	1-1
1.2.1 MasterCard <i>PayPass</i> .....	1-1
1.2.2 Maestro <i>PayPass</i> .....	1-1
1.3 Implementation and Prerequisites Summary .....	1-1
1.4 Transaction Flow Enhancements for <i>PayPass</i> .....	1-2



## 1.1 Product Overview

General information on the *PayPass* product can be found in the documentation section on [www.paypass.com](http://www.paypass.com).

## 1.2 Interoperability

### 1.2.1 MasterCard *PayPass*

The *PayPass*—M/Chip terminal must support both *PayPass*—Mag Stripe and *PayPass*—M/Chip cards. MasterCard *PayPass*—M/Chip cards contain a *PayPass*—Mag Stripe profile which is used for acceptance at *PayPass*—Mag Stripe terminals.

As such, all MasterCard *PayPass* cards and cardholder devices are capable of being accepted by all *PayPass* terminals.

### 1.2.2 Maestro *PayPass*

Maestro *PayPass* is an EMV only implementation and is accepted as Maestro *PayPass* only at *PayPass*—M/Chip terminals.

Maestro *PayPass* cards do not support a *PayPass*—Mag Stripe profile.

## 1.3 Implementation and Prerequisites Summary

Implementing *PayPass*—M/Chip acceptance is an extension to an acquirer's existing infrastructure. The following list is a high-level summary of requirements:

- Acquirers need to start a *PayPass*—M/Chip project with MasterCard and enroll in the *PayPass* program
- Acquirers must support full-grade Contact EMV for all *PayPass*—M/Chip implementations. Partial grade acquiring is not permitted
- Acquirers, or their merchants, will need approved *PayPass* terminals
- Acquirers and merchants must support changes to transaction messages indicating *PayPass* transactions performed at *PayPass* terminals
- Acquirers will need to manage some *PayPass* specific terminal configuration data
- Acquirers must perform the *PayPass*—M/Chip testing

The following chapters detail the acquirer impacts including a summary of the required network changes and terminal data configuration for a *PayPass—M/Chip* implementation.

## 1.4 Transaction Flow Enhancements for *PayPass*

The *PayPass—M/Chip* terminal transaction flow is based on the EMV 4.1 specifications, with the specific *PayPass* adaptations summarized below. The *PayPass* transaction flow is defined in the *PayPass—M/Chip* Technical Specifications.

Transaction processing has been enhanced for *PayPass—M/Chip*. The principal reason for the changes is to reduce the time that the card and terminal need to be in communication. The changes are implemented by the terminal vendor and any resulting impacts have been included in the relevant sections of this document.

The following is a summary of the changes:

- The terminal only performs the first **GENERATE AC** command. Card-terminal interaction stops after the first **GENERATE AC** command
- Offline Personal Identification Number (PIN) is not supported for performance, usability, and security reasons
- Application Selection has been optimized
- Terminals may make use of a pre-defined record structure on cards

MasterCard has defined the adapted transaction flow which must be implemented for *PayPass—M/Chip*. Refer to the current MasterCard *PayPass M/Chip Technical Specifications* for a definition of this flow and its implementation.

Further details of this optimized transaction flow are suggested in the MasterCard *PayPass* Terminal Optimization Guide available from [www.paypass.com](http://www.paypass.com)

# 2

## Acquirer and Merchant Requirements

*This chapter explains the MasterCard requirements for implementing PayPass—M/Chip acceptance.*

2.1 Overview .....	2-1
2.1.1 Program Enrollment .....	2-1
2.1.2 Terminal Selection.....	2-1
2.1.3 Branding.....	2-2
2.1.4 PayPass Readers.....	2-2
2.1.5 Terminal/Reader Environment.....	2-3
2.1.6 Terminal Application – Technical Requirements.....	2-3
2.2 Supporting Other Payment Acceptance Methods at PayPass—M/Chip Terminals .....	2-4
2.2.1 Accepting PayPass—Mag Stripe and Cardholder Devices (non card form factors) .....	2-4
2.2.1.1 MasterCard PayPass.....	2-4
2.3 New Limits used for PayPass—M/Chip.....	2-6
2.3.1 New Contactless Limit Data Items .....	2-6
2.3.1.1 Terminal Contactless Transaction Limit .....	2-6
2.3.1.2 Terminal CVM Required Limit .....	2-6
2.3.1.3 Terminal Contactless Floor Limit.....	2-8
2.3.2 Hard and Soft Limit Implementations .....	2-8
2.4 Transaction Processing.....	2-9
2.4.1 PayPass—M/Chip Transaction Types.....	2-9
2.4.1.1 Reversals .....	2-9
2.4.1.2 Cancellations .....	2-9
2.4.1.3 Refunds.....	2-9
2.4.2 Application Selection and Cardholder Confirmation.....	2-10
2.4.3 Amount Entry at Attended POS.....	2-10
2.4.3.1 Gratuities/“Tips” .....	2-10
2.4.4 Cardholder Verification.....	2-10
2.4.4.1 MasterCard PayPass Cardholder Verification.....	2-10
2.4.4.2 Maestro PayPass Cardholder Verification .....	2-11
2.4.4.3 Offline PIN .....	2-11
2.4.5 Offline Data Authentication Requirements .....	2-11
2.4.6 Service Code Checking.....	2-12

## Acquirer and Merchant Requirements

---

2.4.7 Terminal Risk Management .....	2-12
2.4.7.1 Floor Limit Check – Cumulative Transaction Amount Checking.....	2-12
2.4.7.2 Random Transaction Selection .....	2-13
2.4.7.3 Velocity Checking .....	2-13
2.4.7.4 Exception File Checking .....	2-13
2.4.8 Online/Offline Terminal Requirements.....	2-13
2.4.9 Clearing.....	2-13
2.4.10 Declined Transactions and Issuer Responses .....	2-14
2.4.10.1 Pick-up/Capture Card Responses .....	2-14
2.4.10.2 Online Declines.....	2-14
2.4.10.3 Card Declines .....	2-14
2.4.10.4 “Referrals”/”Call Me” Issuer Responses .....	2-14
2.5 Receipt Printing .....	2-15
2.6 Fallback for <i>PayPass</i> Transactions.....	2-16
2.7 Terminal and Network Performance .....	2-17

## 2.1 Overview

This section describes the Acquirer and Merchant terminal requirements.

### 2.1.1 Program Enrollment

Acquirers implementing *PayPass*—M/Chip acceptance must enroll in the MasterCard *PayPass* program by completing an enrollment form. Program enrollment allows acquirers access to all required specifications and to receive MasterCard related services and products. Only enrolled acquirers may offer their *PayPass* acquiring services or products to cardholders and merchants.

Details of the enrollment can be obtained from MasterCard by sending an email requesting *PayPass* Program Enrollment to [license@paypass.com](mailto:license@paypass.com) or via your local MasterCard representative.

### 2.1.2 Terminal Selection

The following sections provide general information on *PayPass*—M/Chip terminal design and options to help acquirers and/or their merchants select existing or new terminals that meet their business needs. Details of the implementation requirements for all *PayPass* terminals are contained in the MasterCard *PayPass* Terminal Implementation Requirements document available from [www.paypass.com](http://www.paypass.com). All *PayPass*—M/Chip terminals must support MasterCard's branding requirements (See Section 2.1.3) but acquirers and merchants will need to choose their implementation-specific options such as:

- The physical design of the *PayPass*—M/Chip terminal and reader
- Other payment acceptance methods that the implementation supports (at the same or different terminal)
- Terminal and network performance

Acquirers and merchants must only use approved *PayPass* terminals. Products which are not *PayPass* approved will need to obtain approval before implementation. Subsequent changes to terminal software could affect compliance with *PayPass* Terminal Vendor testing and must be discussed with MasterCard.

The vendor procedures for *PayPass* approval are given in the MasterCard *PayPass* Terminal Vendor Testing Process manual. An acquirer need not be involved in the approval process, other than to request proof of approval from the vendor.

Products which are already *PayPass* approved products are listed on [www.paypass.com](http://www.paypass.com).

### **2.1.3 Branding**

Acquirer or merchant terminals must conform to MasterCard brand requirements.

In order to give the cardholder clear information as to where to tap the *PayPass* device on the *PayPass* terminal, MasterCard has created the *PayPass* landing zone to help cardholders locate MasterCard *PayPass* terminals. The landing zone must be placed on the terminal to indicate where the cardholder has to tap or hold the MasterCard *PayPass* card. The landing zone must contain the contactless identifier and if space permits should contain the *PayPass* identifier.

Acceptable designs are described in the following documents:

- *MasterCard PayPass Branding Standards*
- *Maestro PayPass Branding Standards*
- *MasterCard PayPass Terminal Implementation Requirements*

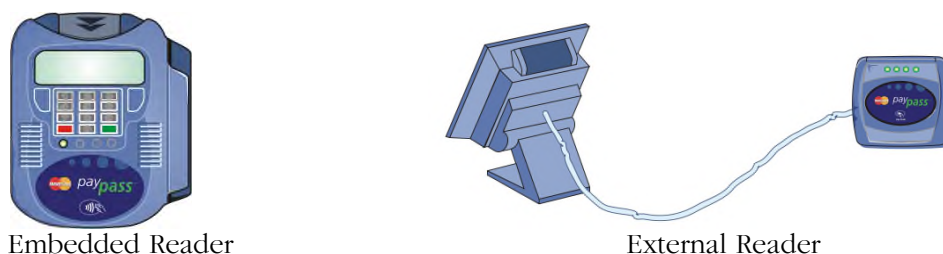
### **2.1.4 PayPass Readers**

*PayPass* contactless card-to-terminal communication is supported by new *PayPass* readers. Acquirers may plan deployment of *PayPass* readers as extensions to an existing Point of Sale (POS) or as new terminal implementations. A *PayPass* reader does not necessarily have to be embedded in the terminal. A *PayPass* reader may be fully or partially integrated into a POS terminal as illustrated in Figure 2.1. The contactless reader may be integrated with the POS equipment in a number of configurations. Acquirers and merchants therefore have a high degree of flexibility on how to implement terminals appropriately.

For example, the *PayPass* reader(s) could be connected to:

- Individual electronic cash registers connected to a merchant store system
- A single central terminal (e.g., in a tollgate or transportation scenario)
- A stand-alone terminal (e.g., video rental store, bus)

Figure 2.1—*PayPass* Readers



## 2.1.5 Terminal/Reader Environment

Acquirers should note the importance of the physical environment for their *PayPass*—M/Chip terminals.

The placement of the *PayPass* reader is particularly important as it is the cardholder who uses the terminal and not the merchant. The *PayPass* reader containing the antenna needs to be conveniently placed and easily visible.

The *PayPass* contactless operation can also be adversely affected by inappropriate placement of the reader; e.g., on a metal surface.

MasterCard recommends that where possible, the *PayPass* readers are included in a PIN Entry/contact card acceptance device keeping the terminal footprint on the merchant site to a minimum.

## 2.1.6 Terminal Application – Technical Requirements

The terminal application for *PayPass*—M/Chip must meet the technical requirements of *PayPass*—M/Chip Technical Specifications. Additional *PayPass*—M/Chip specific application requirements for the terminal application and transaction processing are described in the following sections.

## 2.2 Supporting Other Payment Acceptance Methods at *PayPass*—M/Chip Terminals

As there is no issuer ICC response data in *PayPass*—M/Chip transactions, frequent consecutive use of a *PayPass* card will cause a card's offline counters to accumulate. If the *PayPass* card is not used as a contact EMV card, then the card's limits will finally be exceeded and a contact transaction required. A successful online contact EMV transaction resets the card's offline counters. For further information on how offline counters affect card behavior in M/Chip applications, refer to the M/Chip Requirements manual and the M/Chip Program Guide.

*PayPass*—M/Chip enabled merchant locations must also support contact EMV and magnetic stripe (swipe) acceptance. Contactless only acceptance locations are only allowed by agreement with MasterCard (buses and parking meters are permitted to be contactless only).

The choice to use *PayPass* as a payment method rather than a contact transaction is at the discretion of the cardholder.

### 2.2.1 Accepting *PayPass*—Mag Stripe and Cardholder Devices (non card form factors)

*PayPass*—M/Chip terminals must support *PayPass*—Mag Stripe transactions, if they accept MasterCard.

*PayPass*—Mag Stripe is not supported for Maestro *PayPass*. A *PayPass*—M/Chip terminal accepting Maestro *PayPass* only may support *PayPass*—Mag Stripe but will not be used as Maestro *PayPass* cards do not support the *PayPass*—Mag Stripe profile.



#### Note

**A *PayPass* – M/Chip terminal must terminate the transaction if a *PayPass* Maestro card indicates that it does not support *PayPass* – M/Chip.**

#### 2.2.1.1 MasterCard *PayPass*

Transactions from *PayPass*—Mag Stripe cards and *PayPass* cardholder devices are *PayPass* transactions with the new values in existing fields as described in Chapter 4 of this document.

Merchants must be made aware that *PayPass* acceptance also means that cardholder devices will be valid for acceptance at their terminals. Examples of non card form factors include key fobs and mobile phones (See Figure 2.2)

Figure 2.2— Example Cardholder Devices (Non Card Form Factors)



## 2.3 New Limits used for *PayPass*—M/Chip

*PayPass* introduces new terminal limits. The use of these limits is described in this section.



**Note** Valid implementations of the limits are shown in Appendix A of this document.

### 2.3.1 New Contactless Limit Data Items

New terminal held limits are used in *PayPass*—M/Chip transaction processing at *PayPass*—M/Chip terminals and must be configurable for each AID accepted at the *PayPass*—M/Chip terminals. The following new limits are defined for *PayPass*:

- Terminal Contactless Transaction Limit
- Terminal CVM Required Limit
- Terminal Contactless Floor Limit



**Note** A limit is not exceeded for transactions less than or equal to the MasterCard published values.

#### 2.3.1.1 Terminal Contactless Transaction Limit

The *PayPass* Terminal Contactless Transaction Limit is a maximum transaction amount above which a contactless transaction must not be performed.

#### 2.3.1.2 Terminal CVM Required Limit

As part of the *PayPass* program, MasterCard has introduced new global rules for cardholder verification and receipt requirements. The rules define transaction amounts where cardholder verification and receipts are optional for all *PayPass* transactions less than, or equal to these amounts. The limits are referred to as the “*PayPass* Terminal CVM Required Limit.” *PayPass* transactions equal to, or under the *PayPass* Terminal CVM Required Limit, do not require either cardholder verification or a receipt; however, a cardholder may still request a receipt.

The *PayPass* Terminal CVM Required Limit is applicable only to CVM and receipt processing and is not used to influence decisions to authorize transactions online or offline. At online capable terminals, online authorization may still be required if Terminal Action Analysis results in an ARQC request to the card, or if a card returns an ARQC to a TC request.

The terminal must only support 'No CVM' as the CVM method for *PayPass* transactions below or equal to the MasterCard defined limit.

Online transactions below or equal to the Terminal CVM Required Limit do not require a CVM.

Above the Terminal CVM Required Limit, CVM processing is required as defined in the *PayPass—M/Chip* Technical Specification, and Terminal Action Analysis may result in an online transaction. The CVM to be used is determined by the CVM list supplied by the card and the CVM capabilities of the terminal. If 'online PIN' is the CVM selected method above the *PayPass* CVM limit then transactions will be sent online. This is standard processing according to the MasterCard recommended Terminal Action Code settings.

Transactions above this limit may still be authorized or declined offline if the card or terminal did not require an online authorization, as in standard EMV processing.

For *PayPass* M/Chip transactions below the terminal floor limit, online behavior is determined by either the result of Terminal Action Analysis or a card responding with an ARQC.

Implementations may choose to implement the Terminal Contactless Transaction Limit and the Terminal CVM Required Limit with equivalent values, such that all *PayPass* transactions are 'No CVM'. In this case it is recommended that the terminal also supports contact chip and contact mag stripe transactions.

Below, or equal to the limit:

- *PayPass—M/Chip* - 'No CVM' is the only method supported
- *PayPass—Mag Stripe* - Signature is not required



**Note**

**The CVM limit does not apply to devices which must, by definition, perform cardholder verification—for example CAT 1.**

Above the limit:

*PayPass—M/Chip* – CVM processing is performed according to the CVM List returned by the card and the Terminal Capabilities of the Terminal. *PayPass—Mag Stripe* CVM processing is as current mag stripe rules.

### **2.3.1.3 Terminal Contactless Floor Limit**

The Terminal Contactless Floor Limit is a transaction amount above which issuer authorization is required.

In practice the Terminal Contactless Floor Limit may often be set to the same value as the contact floor limit but terminal implementations should be able to maintain and use this limit independently.

Below, or equal to the limit:

- *PayPass*—M/Chip transactions may be authorized offline if the card approves (returns a TC). The terminal and issuer action codes determine if the card is asked for an offline approval when this limit is exceeded.
- *PayPass*—Mag Stripe transactions must be authorized by the issuer except for specific terminal types allowed to accept offline transactions as defined by the current mag stripe rules.

Above the limit:

- *PayPass*—M/Chip transactions must be authorized by the issuer. The terminal and issuer action codes determine if the card is asked for an online response (ARQC) when this limit is exceeded.
- *PayPass*—Mag Stripe transactions – must be authorized by the issuer except for specific terminal types allowed to accept offline transactions as defined by the current mag stripe rules.

### **2.3.2 Hard and Soft Limit Implementations**

A hard limit implementation is when the Terminal CVM Required Limit is equal to the Terminal Contactless Transaction Limit.

A soft limit implementation is when the Terminal Contactless Transaction Limit is not used, or set to the maximum value.

Hard limit configurations may only be implemented for a whole market or region.

All Maestro *PayPass* implementations are hard limit implementations.

## 2.4 Transaction Processing

### 2.4.1 *PayPass*—M/Chip Transaction Types

Permitted *PayPass*—M/Chip transaction types are as current payment product rules.

The following specific transaction requirements apply to all *PayPass*—M/Chip products:

#### 2.4.1.1 Reversals

Acquirer/system generated reversals for online authorizations are as current processing.

#### 2.4.1.2 Cancellations

Card risk management counters may be adversely impacted if a *PayPass*—M/Chip transaction is cancelled under certain conditions. The following requirements prevent this impact.

A terminal may allow a merchant to cancel a transaction if a transaction has not yet been initiated with the *PayPass*—M/Chip card (i.e. before a **GENERATE AC** command) or the card has requested an online authorization. All transactions that have been approved offline by a *PayPass*—M/Chip card must be submitted in clearing to the issuer. However a merchant may offer a refund against these transactions.

#### 2.4.1.3 Refunds

##### **MasterCard *PayPass* Refunds**

Contactless refunds must be supported for MasterCard *PayPass*.

To prevent card risk management counters being adversely impacted, refunds must be performed by requesting an AAC from the *PayPass*—M/Chip card.

##### **Maestro *PayPass* Refunds**

Refunds are not currently supported as contactless transactions for Maestro *PayPass*. Refunds must be performed as contact transactions and as described in the *M/Chip Requirements* manual.

## 2.4.2 Application Selection and Cardholder Confirmation

*PayPass—M/Chip* terminals do not support cardholder confirmation for *PayPass* contactless transactions. The payment application is selected automatically by the *PayPass—M/Chip* terminal. Acquirers will therefore not need to support the EMV option of allowing cardholders to confirm selection of an application at a *PayPass* terminal.

*PayPass—M/Chip* terminals must support partial name matching during application selection.

*PayPass* card applications that have been personalized to require cardholder confirmation will not be accepted as *PayPass* transactions at *PayPass—M/Chip* terminals.

## 2.4.3 Amount Entry at Attended POS

If a merchant uses a separate Electronic Cash Register (ECR) and *PayPass* POS terminal then they should be connected. The payment amount generated by the ECR should be made automatically available electronically to the *PayPass* terminal when a cardholder chooses to pay with *PayPass*.

The final transaction amount must be known before performing a *PayPass* transaction.

### 2.4.3.1 Gratuities/‘Tips’

If gratuities (tips) are supported then the cardholder must be offered the opportunity to enter the gratuity amount before ‘tapping’.

## 2.4.4 Cardholder Verification

### 2.4.4.1 MasterCard *PayPass* Cardholder Verification

If a terminal supports transactions above the Terminal CVM Required Limit then it must also support the current product rules for CVMs (except offline PIN as explained below). The required CVMs are summarized below:

#### **Attended Terminals**

Signature (Mandatory), No CVM (Mandatory), Online PIN optional.

#### **Unattended Terminals**

CAT1: Online PIN (Mandatory)

CAT2 and CAT3: No CVM (Mandatory)

#### 2.4.4.2 Maestro *PayPass* Cardholder Verification

Terminals accepting Maestro *PayPass* must support 'No CVM'.

#### 2.4.4.3 Offline PIN

Offline PIN is not supported at *PayPass*—M/Chip terminals for *PayPass*—M/Chip transactions. Offline PIN may be supported at the same terminal but only for contact EMV transactions.

*PayPass*—M/Chip does not support offline PIN verification over the contactless interface. Both offline plaintext PIN and offline enciphered PIN verification are not available when using the *PayPass* technology. The reasons for not supporting offline PIN are:

- A practical difficulty of asking cardholders to enter a PIN while holding the card in front of the reader.
- A potential security vulnerability from eavesdropping and PIN probing.

Preventing offline PIN support requires a specific definition of the Terminal Capabilities in the configuration data for a *PayPass*—M/Chip terminal, as defined in Section 3.6 of this document.

### 2.4.5 Offline Data Authentication Requirements

The following requirements apply to *PayPass*—M/Chip transactions only. Data authentication requirements for contact EMV transactions remain unchanged. Data authentication requirements are defined in the MasterCard *PayPass*—M/Chip Technical specification.

The terminal's payment system public keys for *PayPass*—M/Chip are the same values as for contact EMV and may be shared with a contact application for *PayPass* use.

*PayPass*—M/Chip terminals must support data authentication for MasterCard and Maestro *PayPass* as shown in Table 2.1.

**Table 2.1— Offline Data Authentication Requirements for MasterCard and Maestro *PayPass* at *PayPass*—M/Chip Terminals**

	Offline Static Card Authentication Method (CAM)	Offline Dynamic CAM	
	SDA	DDA	CDA
Attended POS and CAT with offline capability. (Includes offline-only POS & CAT)	Mandatory (If terminal supports MasterCard, else n/a for Maestro)	Optional	Mandatory
Online-only POS & CAT	Optional	Optional	Optional

## 2.4.6 Service Code Checking

Terminals must be able to determine when transaction data has been obtained using a contactless interface. Terminals must not prompt for a contact transaction when the service code of a *PayPass* transaction indicates a chip is present on the card, except following a card declined transaction (see section 2.4.10.3).

For *PayPass*-M/Chip transactions the service code must not be used to require online authorization or online PIN.

For *PayPass*—Mag Stripe transactions, the service code must not be used to require online PIN below or equal to the Terminal CVM Required Limit.



### Note

**Acquirers or their terminal must not reject or otherwise decline to complete a transaction solely because of the service code encoded in Track 2. If cardholder verification is required and a service code indicates that online PIN is required but the terminal does not support online PIN, then the terminal must send the transaction to the issuer for authorization without the online PIN.**

## 2.4.7 Terminal Risk Management

The following are specific requirements applicable to terminal risk management for *PayPass*.

### 2.4.7.1 Floor Limit Check – Cumulative Transaction Amount Checking

EMV defines an optional floor limit check that may be performed by terminals. This optional check allows terminal stored transaction value per card to be accumulated and the result to be used for the floor limit check.

*PayPass* terminals must not use an accumulated transaction amount by card for the purpose of checking if the floor limit is exceeded.

#### **2.4.7.2 Random Transaction Selection**

This EMV check must not be performed for *PayPass* transactions.

#### **2.4.7.3 Velocity Checking**

This EMV check must not be performed for *PayPass* transactions.

#### **2.4.7.4 Exception File Checking**

This EMV function is optional in the terminal for *PayPass*—M/Chip transactions.

### **2.4.8 Online/Offline Terminal Requirements**

The following sections describe online/offline authorization requirements. <sup>1</sup>

*PayPass* M/Chip terminals (except CAT3) must have online capability or the ability to obtain issuer authorization before clearing, and may also support offline transactions.

As some issuer card products may be configured to work as offline only, MasterCard recommends that, where possible, online capable terminals are configured to be offline capable for transactions below the *PayPass* limits.

*PayPass*—Mag Stripe transactions must be authorized by the issuer.

### **2.4.9 Clearing**

Clearing requirements are as current product rules. The new *PayPass* data values are summarized in chapter 4 of this document.

---

<sup>1</sup> A transaction that is required to be “online authorized” means “authorized by the issuer before submission of the financial transaction”. In most cases this will be with an online real time authorization to the issuer.

## 2.4.10 Declined Transactions and Issuer Responses

### 2.4.10.1 Pick-up/Capture Card Responses

Acquirers must decline transactions with a 'Decline and Pick Up/Capture Card' response. Retaining the card at an attended terminal is optional as it may be impractical for an attendant to retain a card that is not initially handed over to the merchant during payment.

### 2.4.10.2 Online Declines

Following an online decline, (Not Authorized) there is no restriction on performing a subsequent contact transaction, if supported by the terminal.

### 2.4.10.3 Card Declines

Following a card decline (AAC Response), the terminal must prompt the cardholder to perform a contact transaction, if supported by the terminal and the terminal did not request a card decline.

### 2.4.10.4 "Referrals"/"Call Me" Issuer Responses

"Referrals"/"Call Me" Issuer responses are not required to be supported by Acquirers for *PayPass*—M/Chip. Referral responses may be declined by the Acquirer or Merchant.

## 2.5 Receipt Printing

Current product rules and any legal requirements determine if this option must still be provided on request.

Fast receipt printing is recommended for cardholders requesting a receipt, or transactions above the *PayPass* Terminal CVM Required Limit.

*PayPass* receipts may be offered at the end of a transaction, upon cardholder request, rather than the cardholder or merchant needing to confirm if they would like a receipt before continuing.

An example solution could be to offer a 'Print Receipt' function or button for the cardholder or merchant, allowing a receipt to be printed up until the next transaction is started. Alternatively, the terminal may propose to print a receipt, and if there is no positive action from the merchant within X seconds, the receipt printing is cancelled automatically.



### Note

**If a terminal supports contactless transactions above the Terminal CVM Required Limit then it must support receipt printing for Signature CVM.**

## 2.6 Fallback for *PayPass* Transactions

The following defines the *PayPass* requirements for technical fallback at *PayPass* terminals.

A *PayPass* technical fallback transaction is a consecutive transaction, at the same terminal, with the same card (or cardholder device) but with a different acceptance technology (for example., contact EMV or mag stripe). Transactions are classified as technical fallback when the preceding transaction did not complete because of a technical failure in the terminal-to-card communication after the first successful select command. Application layer errors or declines are not considered communication errors. A consecutive transaction with the same card at a different terminal is not considered a *PayPass* fallback transaction.

If a *PayPass* transaction fails (as described above) then a new transaction may be attempted, if supported by both the card and the terminal in the order of preference of:

1. Contact EMV
2. Magnetic stripe (swipe)

*PayPass* technical fallback transactions are authorized according to the current payment product rules. There are no changes to network messages for identifying *PayPass* technical fallback. Current rules apply to transactions falling back from contact to mag stripe. Current rules for fallback with contact EMV are explained in the *M/Chip Requirements*.

There are no changes to authorization requirements for *PayPass* fallback transactions. *PayPass* fallback transactions are authorized according to the current payment product rules.

## 2.7 Terminal and Network Performance

The *PayPass* product emphasizes:

- Cardholder convenience
- Adoption of card payments for lower value transactions
- Fast transactions

The adoption of card payments for lower value transactions is likely to increase the volume of card transactions. The acquirer/merchant terminals and their networks should plan for an increased volume of transactions. Increased use of *PayPass*—M/Chip may also result in a corresponding rise in the number of contact EMV transactions at the same or other terminals for the reasons described in Section 2.2.

Required transaction timings may vary significantly depending upon the type of deployment and factors external to the terminal (for example, network and host system capabilities). Acquirers and merchants should assess their choice of terminal and the implementation environment with consideration to:

- Speed of offline data authentication (for example, for Combined Data Authentication (CDA), Dynamic Data Authentication (DDA), Static Data Authentication (SDA) and with varying key lengths and a variation of cards).
- Normal<sup>2</sup> online response times for online capable terminals; from determining that an online authorization is required to receiving the online authorization response, including the establishing of the online connection, should be equal to or less than ¼ seconds. Acquirers may need to ensure that dedicated high speed connections are implemented to meet these response times.

---

<sup>2</sup> Average time where no communications or host system problems are encountered



# 3

## Terminal Configuration Data

*This chapter provides further information on how to configure PayPass—M/Chip specific data based on the requirements in Chapter 2.*

---

3.1 PayPass—M/Chip Specific Terminal Data.....	3-1
3.2 AIDs and Related Application Labels .....	3-2
3.3 Application Version Number .....	3-4
3.4 PayPass Limits .....	3-4
3.4.1 Maestro PayPass Limits .....	3-4
3.4.2 MasterCard PayPass—M/Chip Limits .....	3-4
3.4.2.1 Terminal Contactless Transaction Limit .....	3-5
3.4.2.2 Terminal CVM Required Limit .....	3-5
3.4.2.3 Terminal Contactless Floor Limit.....	3-5
3.5 Terminal Action Codes (TACs).....	3-6
3.5.1 Terminal Action Codes - Online Capable Terminals .....	3-7
3.5.2 Terminal Action Codes - Offline Only Terminals (CAT3) .....	3-9
3.6 Terminal Capabilities.....	3-11
3.7 Terminal Type .....	3-12



### 3.1 *PayPass—M/Chip* Specific Terminal Data

The following sections provide configuration requirements for *PayPass—M/Chip* terminals.

The acquirer and/or merchant must ensure that the following are *PayPass—M/Chip* specific and maintainable independently of other contact EMV data:

- List of Application Identifiers (AIDs) and related application labels supported for contactless acceptance
- For each of the above AIDs:
  - Terminal Contactless Transaction Limit
  - Terminal CVM Required Limit
  - Terminal Contactless Floor Limit
  - Permitted Transaction Types
  - Terminal Action Codes

The *PayPass* requirements for the following data items are also defined for *PayPass—M/Chip* terminals. They are not required to be *PayPass* specific. For example they may additionally reflect the configuration of the combined contact and contactless device.

- Terminal Capabilities
- Terminal Type

## 3.2 AIDs and Related Application Labels

*PayPass*—M/Chip terminals must maintain an independent list of application identifiers (AIDs) accepted by the terminal for *PayPass*. The AID value used for transaction processing is the AID of the card application—for example, MasterCard Credit (A0000000041010). There are no specific AIDs for *PayPass*. The terminal list of identifiers is a list of all applications accepted at that terminal. PIX extensions should only be used for specific domestic, co-branding or issuer implementations. Generic acceptance of *PayPass* cards uses the product AID without any extension. Table 3.1 provides the names (Application Labels) that must be associated with the specific AIDs used for MasterCard products.

**Table 3.1— AIDs and Related Application Labels**

PRODUCT	RID	PIX	PIX EXTENSION	APPLICATION LABEL
MasterCard*	A000000004	1010	—	“MasterCard”
MasterCard with domestic functions	A000000004	1010	DCCC XX..	“MasterCard”
MasterCard applications for domestic environment only	A000000004	9999	DCCC XX...	Issuer-defined
MasterCard co-branded	A000000004	1010	CNNNNN YYYY..	“MasterCard”
Maestro	A000000004	3060		“Maestro”
Maestro with domestic functions	A000000004	3060	DCCC XX..	“Maestro”
Maestro co-branded with a club	A000000004	3060	CNNNNN YYYY..	“Maestro”

*\*For cards with a single payment application, the ‘MasterCard’ AIDs apply to both Debit and Credit products. The application label for Debit MasterCard is ‘Debit MasterCard’.*

### Legend

D: Hex “D” (4 bits coded as 1101)

C: Hex “C” (4 bits coded as 1100)

CCC: Country code of the national registration authority

NNNN: Co-brander's identification defined by MasterCard

XX: Defined by the national registration authority

YYYY: Defined by the co-brander

As defined by ISO 7816-5, domestic schemes may use the registration category "D" (4 bits coded as 1101) followed by the country code of the national registration authority, followed by fields specified by the national authority. This may be used for cards with a non-MasterCard Issuer Identification Number (IIN). Table 3.1 lists the application label recommended by MasterCard. Issuers and acquirers can either use the labels in lowercase (for example, "mastercard"), as provided in Table 3.1, or in capitals (for example, "MASTERCARD").



**Note**

***PayPass—M/Chip terminals must permit partial name matching for these AIDs. This means that AIDs longer than these specific AIDs must also be considered as a successful match.***

### 3.3 Application Version Number

The terminal application version numbers for *PayPass—M/Chip* is defined as follows:

*PayPass—M/Chip* Terminal = '0002'

### 3.4 *PayPass* Limits

The required values for *PayPass* limits are agreed by MasterCard at a market or regional level. They are published in:

- *Chargeback Guide— (MasterCard PayPass)*
- *Maestro Global Rules (Maestro PayPass)*



**Note**

**It is important to note that the interim updates to these manuals are communicated in Operations Bulletins, which should also be referenced for the latest information.**

Functional implementations of the limits are shown in Chapter 6 of this document.

#### 3.4.1 *Maestro PayPass* Limits

*Maestro PayPass* are hard limit implementations.

The following limits must be the same value for *Maestro PayPass*:

- Terminal Contactless Transaction Limit
- Terminal CVM Required Limit

Collectively they are referred to as the Ceiling Limit in the *Maestro Global Rules*.

- The Terminal Contactless Floor Limit must be equal to, or lower, than the limits above.

#### 3.4.2 *MasterCard PayPass—M/Chip* Limits

The limits published in the *Chargeback Guide* are defined and published as 'Chargeback Protection' amounts. It is these amounts that are equivalent to the Terminal CVM Required Limit. The other limits are not currently referenced in

the *Chargeback Guide*, but are defined in this document and the *PayPass—M/Chip Technical Specifications*.

### 3.4.2.1 Terminal Contactless Transaction Limit

For MasterCard *PayPass—M/Chip* in a soft limit market the Terminal Contactless Transaction Limit must be either not used or set to the maximum value.

For Maestro *PayPass*, and MasterCard *PayPass—M/Chip* in a hard limit market or regional implementation, the Terminal Contactless Transaction Limit must be equal to the Terminal Contactless CVM Required Limit.



**Note**

**Hard limit implementations only apply to a whole region or market.**

### 3.4.2.2 Terminal CVM Required Limit.

As published in the *Chargeback Guide*.

### 3.4.2.3 Terminal Contactless Floor Limit

Unless otherwise specified by MasterCard the Terminal Contactless Floor Limit must be set to either the Terminal Contactless Transaction Limit or current product floor limits, whichever is lower. Online only terminals may implement a zero Terminal Contactless Floor Limit.

## 3.5 Terminal Action Codes (TACs)

TACs specific to *PayPass—M/Chip* use are required per product.

The TACs defined in these tables are specified to work in conjunction with the *PayPass* transaction flows as defined in the MasterCard *PayPass—M/Chip* Technical Specifications. They are optimized with a bias toward permitting offline transactions.

Table 3.2 and Table 3.3 list the defined TACs by terminal type for:

- Online-capable POS and CAT
- Offline-only CAT3



**Note**

**These TACs are specific to *PayPass—M/Chip* terminals performing *PayPass—M/Chip* transactions. If the terminal supports contact transactions the terminal should maintain the *PayPass* TACs independently. They apply to both MasterCard *PayPass* and Maestro *PayPass*.**

### 3.5.1 Terminal Action Codes - Online Capable Terminals

**Table 3.2—MasterCard and Maestro *PayPass* Terminal Action Codes for Online Capable Terminals**

Byte/Bit	Meaning	Denial	Online	Default
1/8	Offline Data Authentication was not performed	0	1	1
1/7	Offline SDA failed	0	1	1
1/6	ICC data missing	0	0	0
1/5	ICC on Hot Card File	0	0	0
1/4	Offline DDA failed	0	1	1
1/3	Combined DDA/AC Generation failed	0	1	1
1/2	Reserved	0	0	0
1/1	Reserved	0	0	0
	<b>HEX VALUE</b>	<b>00</b>	<b>CC</b>	<b>CC</b>
2/8	ICC & Term have different Application Version. Numbers.	0	0	0
2/7	Expired application	0	1	1
2/6	Application not yet effective	0	0	0
2/5	Service not allowed for card product	0	1	1
2/4	New Card	0	0	0
2/3	Reserved	0	0	0
2/2	Reserved	0	0	0
2/1	Reserved	0	0	0
	<b>HEX VALUE</b>	<b>00</b>	<b>50</b>	<b>50</b>
3/8	Cardholder verification failed	0	1	1
3/7	Unrecognized CVM	0	0	0
3/6	PIN try limit exceeded	0	0	0
3/5	PIN entry required but PIN pad not present/not working	0	0	0
3/4	PIN required, PIN pad present but PIN not entered	0	0	0
3/3	On-line PIN entered	0	1	1
3/2	RFU	0	0	0
3/1	RFU	0	0	0

**Terminal Configuration Data**  
**Terminal Action Codes (TACs)**

Byte/Bit	Meaning	Denial	Online	Default
	<b>HEX VALUE</b>	<b>00</b>	<b>84</b>	<b>84</b>
4/8	Transaction exceeds floor limit*	0	1	1
4/7	LCOL exceeded	0	0	0
4/6	UCOL exceeded	0	0	0
4/5	Randomly selected for on-line processing	0	0	0
4/4	Merchant forced transaction on-line	0	1	1
4/3	RFU	0	0	0
4/2	RFU	0	0	0
4/1	RFU	0	0	0
	<b>HEX VALUE</b>	<b>00</b>	<b>88</b>	<b>88</b>
5/8	Default TDOL used	0	0	0
5/7	Issuer authentication unsuccessful	0	0	0
5/6	Script failed before final cryptogram	0	0	0
5/5	Script failed after final cryptogram	0	0	0
5/4	RFU	0	0	0
5/3	RFU	0	0	0
5/2	RFU	0	0	0
5/1	RFU	0	0	0
	<b>HEX VALUE</b>	<b>00</b>	<b>00</b>	<b>00</b>

*\*For the current transaction only. Separate transactions must not be accumulated.*

**Summary of values**

Denial: 00 00 00 00 00

Online: CC 50 84 88 00

Default: CC 50 84 88 00

**Legend**

0: Mandated setting

0/1: Non-mandated setting, dependent upon on the specific terminal configuration.

1: Mandated setting

RFU: Reserved for future use (The settings must be “0, 0, 0”)

### 3.5.2 Terminal Action Codes - Offline Only Terminals (CAT3)

**Table 3.3— MasterCard and Maestro PayPass Terminal Action Codes for Offline Only Terminals**

Byte/Bit	Meaning	Denial	Online	Default
1/8	OfflineData Authentication was not performed	1	0	0
1/7	Offline SDA failed	0	0	0
1/6	ICC data missing	0	0	0
1/5	ICC on Hot Card File	1	0	0
1/4	Offline DDA failed	1	0	0
1/3	Combined DDA/AC Generation failed	1	0	0
1/2	Reserved	0	0	0
1/1	Reserved	0	0	0
	<b>HEX VALUE</b>	<b>9C</b>	<b>00</b>	<b>00</b>
2/8	ICC & Term have different Application Version. Numbers.	0	0	0
2/7	Expired application	1	0	0
2/6	Application not yet effective	0	0	0
2/5	Service not allowed for card product	1	0	0
2/4	New Card	0	0	0
2/3	Reserved	0	0	0
2/2	Reserved	0	0	0
2/1	Reserved	0	0	0
	<b>HEX VALUE</b>	<b>50</b>	<b>00</b>	<b>00</b>
3/8	Cardholder verification failed	1	0	0
3/7	Unrecognized CVM	0	0	0
3/6	PIN try limit exceeded	0	0	0
3/5	PIN entry required but PIN pad not present/not working	0	0	0
3/4	PIN required, PIN pad present but PIN not entered	0	0	0
3/3	On-line PIN entered	1	0	0
3/2	RFU	0	0	0
3/1	RFU	0	0	0

**Terminal Configuration Data**  
**Terminal Action Codes (TACs)**

Byte/Bit	Meaning	Denial	Online	Default
	<b>HEX VALUE</b>	<b>84</b>	<b>00</b>	<b>00</b>
4/8	Transaction exceeds floor limit*	1	0	0
4/7	LCOL exceeded	0	0	0
4/6	UCOL exceeded	0	0	0
4/5	Randomly selected for on-line processing	0	0	0
4/4	Merchant forced transaction on-line	1	0	0
4/3	RFU	0	0	0
4/2	RFU	0	0	0
4/1	RFU	0	0	0
	<b>HEX VALUE</b>	<b>08</b>	<b>00</b>	<b>00</b>
5/8	Default TDOL used	0	0	0
5/7	Issuer authentication unsuccessful	0	0	0
5/6	Script failed before final cryptogram	0	0	0
5/5	Script failed after final cryptogram	0	0	0
5/4	RFU	0	0	0
5/3	RFU	0	0	0
5/2	RFU	0	0	0
5/1	RFU	0	0	0
	<b>HEX VALUE</b>	<b>00</b>	<b>00</b>	<b>00</b>

*\*For the current transaction only. Separate transactions must not be accumulated.*

**Summary of values**

Denial: 9C 50 84 08 00

Online: 00 00 00 00 00

Default: 00 00 00 00 00

**Legend**

0: Mandated setting

0/1: Non-mandated setting, dependent upon on the specific terminal configuration.

1: Mandated setting

RFU: Reserved for future use (The settings must be “0, 0, 0”)

## 3.6 Terminal Capabilities

The Terminal Capabilities field is coded according the definition in *EMV Book 4*.

*PayPass* terminals must use ‘No CVM’ for transactions equal to, or under, the Terminal CVM Required Limit when performing a *PayPass—M/Chip* transaction. Transactions above this limit must perform CVM processing as specified in *EMV 4.1 Book 3*.

The Terminal Capabilities may be specific to *PayPass* or reflect the overall capabilities of the terminal (for example, where the terminal supports both contact and contactless).

If Terminal Capabilities is defined, or used specifically for *PayPass*, then the requirements defined in Table 3.4 apply.



**Note**

**Attended terminals that perform contactless transactions above the CVM limit must support Signature and may support online PIN.**

**Table 3.4— Terminal Capabilities for PayPass**

Byte/Bit	Meaning	Requirement
Byte 2 Bit 8	‘Plain-text PIN for ICC verification’	Must be = ‘0’ (if not supported for contact)
Byte 2 Bit 5	‘Enciphered PIN for offline verification’	Must be = ‘0’ (if not supported for contact)
Byte 2 Bit 4	‘No CVM Required’	Must be = ‘1’

## **3.7 Terminal Type**

The terminal type for *PayPass*—M/Chip terminals may reflect the overall terminal configuration (for example, for a terminal supporting Contact and Contactless).

The terminal type must indicate online capability unless it is a CAT3 terminal.

---

# 4

## Network Interfaces and Host Systems

*This chapter summarizes the impacts and changes to network and host system interfaces.*

---

4.1 Summary of Changes .....	4-1
4.2 Authorization Requests .....	4-2
4.3 Authorization Responses.....	4-4
4.4 Clearing.....	4-4
4.5 Chargebacks .....	4-6
4.5.1 MasterCard Chargebacks.....	4-6
4.5.2 Maestro Chargebacks .....	4-7



## 4.1 Summary of Changes

*PayPass* transactions at *PayPass—M/Chip* terminals are indicated by new values in existing fields for authorizations and clearing. These *PayPass* specific changes are detailed in the *MasterCard Global Operations Bulletin No. 6*, June 2005, and incorporated in the latest authorization and clearing manuals for your region.

*PayPass* transactions from *PayPass—M/Chip* terminals will be either:

- *PayPass* ICC transactions with ICC related data (field DE055 “ICC related Data” and DE023 “Card Sequence Number”—if provided by the card to the terminal)
- *PayPass—Mag Stripe* transactions with the same format as current mag stripe transactions

All *PayPass* transactions contain new values in fields DE022 and DE061, indicating that they are *PayPass* transactions at a *PayPass* terminal.

Acquirers who deploy *PayPass—M/Chip* terminals supporting contact EMV must be Full Grade acquirers. If a *PayPass—M/Chip* terminal accepts contact EMV then it must also accept mag stripe transactions and be EMVCo certified.

Partial Grade and *PayPass—Mag Stripe* acquirers must migrate to Full Grade EMV acquiring.

Full Grade acquiring is the term used to describe an acquirer that has invested in chip terminals, and has also upgraded its network and host systems to support the additional information generated during a chip transaction. Full Grade acquirers provide DE055 in the authorization request messages.

The network changes to support these requirements are summarized in the following sections.

## 4.2 Authorization Requests

*PayPass* authorizations must be processed with the new values in existing fields as defined in Table 4.1 and Table 4.2.

**Table 4.1— New Values in Existing Fields, by Product, for *PayPass* Authorizations**

Product and Transaction Profile	Permitted Values			
	DE022 SE 1	DE023	DE055	DE061
MasterCard	91	n/a	n/a	3 or 4
<i>PayPass</i> —Mag Stripe				
MasterCard <i>PayPass</i> —M/Chip	07	Present if Tag '5F34' is present on card	Mandatory	3
Maestro <i>PayPass</i> —M/Chip	07	Present if Tag '5F34' is present on card	Mandatory	3

**Legend:**

n/a: Not Applicable

**Table 4.2— Defintion of the New Values in Existing Fields for *PayPass* Authorizations**

Data Element	DE022 (POS entry mode)	DE023 (card sequence number)	DE055 (ICC system related data)	DE061 (POS data)
Sub element	SE 1 (POS terminal PAN entry mode)			*SE 11 (POS card data terminal input capability)
Sub element Value and Meaning ( <i>PayPass</i> )	91: PAN auto-entry via contactless mag stripe  07: PAN auto entry via contactless M/Chip	As current definition	As current definition	4: contactless mag stripe  3: contactless M/Chip



**Note**

**Value 3 of DE61se11 is used for any transaction using a contactless chip terminal.**

**Value 4 of DE61se11 is used for any transaction using a contactless mag stripe terminal.**

**This means that value is based on terminal capability, not the transaction.**

## 4.3 Authorization Responses

ICC response data, including Issuer Scripts, is not returned from issuers for *PayPass—M/Chip* transactions. In the event that ICC response data is returned, acquirers are not required to return it to the terminal. If the data is returned to the terminal then the terminal shall not process the data. The terminal is not required to retain the data.

## 4.4 Clearing

New values in existing fields are required for *PayPass* clearing transactions. Table 4.3 and Table 4.4 define the new values and the use of these values by product. Other fields and values remain as present.

**Table 4.3— New Values in Existing Fields, by Product, for *PayPass* Clearing**

Product and Transaction profile	Permitted Values				
	DE022	DE022	DE022	DE023	DE055
	SE 1	SE 7	SE 10		
MasterCard <i>PayPass—Mag Stripe</i>	A or M	A	3 or 0	n/a	n/a
MasterCard <i>PayPass—M/Chip</i>	M	M	3 or 0	Present if Tag '5F34' was present from card	Mandatory <sup>1</sup>
Maestro <i>PayPass—M/Chip</i>	M	M	3 or 0	Present if Tag '5F34' was present from card	Mandatory <sup>2</sup>

### Legend

n/a: Not Applicable

<sup>1</sup> DE055 is mandatory in clearing for Europe acquirers only. For non-Europe acquirers it is mandatory from 1/1/2011.

<sup>2</sup> DE055 is mandatory in clearing for Europe acquirers only. For non-Europe acquirers it is mandatory from 1/1/2011.

**Table 4.4— Definition of the New Values in Existing Fields for *PayPass* Clearing**

Data Element	DE022 (POS entry mode)	DE022 (POS entry mode)	DE022 (POS entry mode)	DE023 (card sequence number)	DE055 (ICC system related data)
Sub element	SE 1 (POS card data input capability)	7 (card data input mode)	10 (card data output capability)		
Sub element Value and Meaning ( <i>PayPass</i> )	A: terminal supports PAN auto-entry via contactless mag stripe M: terminal supports PAN auto-entry via contactless M/Chip	A: PAN auto-entry via contactless mag stripe M: PAN auto entry via contactless M/Chip	0: unknown no indication given 1: none 3: ICC (Contact EMV, <i>PayPass</i> —Mag Stripe, and <i>PayPass</i> —M/Chip)	As current definition	As current definition



**Note**

**Value 3 of DE61se11 is used for any transaction using a contactless chip terminal.**

**Value 4 of DE61se11 is used for any transaction using a contactless mag stripe terminal.**

**This means that the value is based on terminal capability, not the transaction.**

## 4.5 Chargebacks

### 4.5.1 MasterCard Chargebacks

Cardholder verification and receipts are optional for all *PayPass* transactions under a defined global amount (currently US \$25 or 25 Euro), or the locally set amount for that country or region. The applicable amount for each country or region can be found in appendix D of the *Chargeback Guide* (referred to as a “chargeback protection amount”). These implementation requirements refer to the transaction amount at which the new requirement applies as the “*PayPass* Terminal CVM Required Limit” (See also Section 2.4.4.3 of this document).

To support this change, acquirers are protected against chargebacks for *PayPass* transactions with the reason codes shown in Table 4.5. Issuers may not chargeback properly identified *PayPass* transactions with these reason codes.

**Table 4.5—*PayPass* Impacted Chargeback Reason Codes**

Message Reason Code	Description
4801	Requested Transaction Data Not Received
4802	Requested/Required Information Illegible or Missing
4837	No Cardholder Authorization

Full details of the impacted chargeback message reason codes are available in Section 2.12 of the *MasterCard Chargeback Guide*.

For users of MasterCom, the existing Acquirer’s Retrieval Response Code has been updated to reflect these changes (see Table 4.6). Acquirers may use this rejection code for qualified *PayPass* transactions under the defined global amount (currently US \$25 or 25 Euro), or the country or region specific amount as published in appendix D of the *MasterCard Chargeback Guide*.

**Table 4.6— Updated MasterCom Acquirer Response Codes for *PayPass***

Acquirer Response Code	Description
C	The issuer’s request for retrieval was for a transaction identified as a <i>PayPass</i> transaction that is equal to or below ... (refer to the current value in the Chargeback Guide)  or  QPS—No item available

Full details of the impacted acquirer response code is available in Section 6.3.2 of the *MasterCard Chargeback Guide*

## 4.5.2 Maestro Chargebacks

Maestro chargeback rules have been updated to include Maestro *PayPass*. No new reason codes have been introduced. Updates to the existing reason codes are documented in the *Maestro Global Product Rules*.



# 5

## Testing

*This chapter provides an overview of the testing process required for PayPass—M/Chip implementation.*

---

5.1 Testing Overview .....	5-1
5.2 Testing Scope by <i>PayPass</i> Terminal Type .....	5-1
5.3 Testing Process .....	5-1
5.4 Test Stages .....	5-2
5.5 NIV .....	5-3
5.5.1 Offline Authorization Testing (Mandatory) .....	5-3
5.5.2 Conditional Offline Clearing Testing .....	5-3
5.5.3 Optional Online Testing .....	5-3
5.6 TIP .....	5-4
5.7 ETED .....	5-5
5.8 Post-Live Monitoring .....	5-5
5.9 Further Information and Contact Details.....	5-6



## 5.1 Testing Overview

The MasterCard test process for *PayPass—M/Chip* is a series of test stages.

This chapter summarizes how *PayPass—M/Chip* implementations are tested. Acquirers will be able to use this information to plan their testing and understand the purpose, scope, and requirements for *PayPass* testing. Refer to the *PayPass* specific testing documentation for more information.

This guide is for acquirers who are already contact EMV acquirers.

Only the additional testing for *PayPass—M/Chip* is described here. For more information on migrating to contact EMV refer to the *MasterCard M/Chip Implementation Guide*.

## 5.2 Testing Scope by *PayPass* Terminal Type

The acquirer or merchant's choice of terminal determines the scope of required testing. All new *PayPass—M/Chip* implementations must perform this testing.

In addition, if the terminal also supports contact EMV then:

- The terminal must be EMV certified
- TIP for a new contact EMV terminal must be performed

An acquirer who has already implemented *PayPass—M/Chip* and is only adding new terminals must only perform:

- TIP for a new *PayPass—M/Chip* terminal
- TIP for a new contact EMV terminal if the terminal supports contact EMV and the terminal must be EMV certified

Information on contact EMV testing is available in the *MasterCard M/Chip Customer Implementation Guide*.

## 5.3 Testing Process

The services provided by MasterCard and described in this section are designed to validate, to a reasonable degree, that the acquirer's infrastructure can accept MasterCard *PayPass* approved cards.

## 5.4 Test Stages

This testing section applies to both Maestro *PayPass* and MasterCard *PayPass* unless specifically stated.

The acquirer test stages for a *PayPass*—M/Chip implementation are summarized in Table 5.1. The following sections provide a summary of each stage. The stages are then further explained in the following sections.

**Table 5.1— Summary Test Stages**

Stage	Required	Description and Notes
NIV (Network Interface Validation)	Required(Once per acquirer or processor)	Purpose: Tests the acquirer authorization and clearing network interfaces against the MasterCard simulators, using ETEC cards.  Additional <i>PayPass</i> transactions have been added.
TIP (Terminal Integration Process)	Required	Purpose: Tests the terminal in an integrated acquirer environment.  The TIP tests to be performed are defined when the acquirer supplies MasterCard with a completed TIP questionnaire. Relevant ETEC cards are used with the acquirer terminal(s).
End-to-End Demonstration (ETED)	Required	Purpose: Validates the completed implementation in the production environment, including some areas that can only be validated in production (for example, key management and network functions.)  A set of <i>PayPass</i> transactions are performed by MasterCard using MasterCard-supplied live cards.
Post Live Monitoring	Required	Purpose: Monitor the stability of the implementations through normal business use.  No acquirer action required.

---

## 5.5 NIV

Acquirers run the tests and then submit log files from the simulators for validation by MasterCard.

To correctly process *PayPass* transactions, acquirers need to upgrade their network interfaces with MasterCard. The NIV testing checks that authorization and clearing interfaces are in accordance with the current MasterCard authorization and clearing requirements for the acquirer's region.

Subset 6 and 7 ETEC cards are used with the MasterCard simulator for this testing.

### 5.5.1 Offline Authorization Testing (Mandatory)

For authorization testing, acquirers use the MasterINQ Simulator (U.S. region), or the MasterCard Europe Authorization Simulator (MEAS) (non-U.S. regions) to ensure that they are able to correctly provide the additional chip data in authorization messages.

With the simulator connected to the acquirer host, which is itself connected to the terminal, acquirers perform transactions using the ETEC cards. Further explanations regarding ETEC cards are also provided in the *MasterCard M/Chip Implementation Guide*.

### 5.5.2 Conditional Offline Clearing Testing

Currently, acquirers must send chip data in clearing messages. Acquirers that do decide to send chip data in clearing messages must perform offline clearing testing before being set up for live operations. Acquirers performing clearing testing use the MasterCard Clearing Presentment Simulator to validate the:

- Conformity of the clearing interface
- Ability of the host system to send clearing messages containing chip data

### 5.5.3 Optional Online Testing

Online testing is optional. Acquirers that wish to perform online tests must interface with the online testing facility provided by MasterCard.

The online testing facility provides the following benefits:

- Availability of a close-to-production environment, where the bank sends real messages across the real network infrastructure

- Ability to perform specific testing customized to meet the needs of the acquirer

NIV should be completed, or very near to completion before beginning TIP Testing.

## 5.6 TIP

Acquirers run the tests and then submit log files from the simulators for validation by MasterCard.

The TIP is designed to validate that the terminal:

- Meets the business needs of the acquirer
- Conforms to the MasterCard *PayPass*—M/Chip and *PayPass*—Mag Stripe Technical Specifications and this document, after integration in the acquirer environment

Conforms to MasterCard requirements related to the:

- Payment product(s) the terminal will accept (such as the support of online PIN, if required)
- Operational effectiveness, such as the implementation of “fallback to contact or magnetic stripe” (depending on the terminal type)

Based on the needs of the acquirer, the TIP can comprise up to four components:

1. A validation that the terminal meets the requirements of both the acquirer and MasterCard.
2. An assessment of testing requirements and identification of the ETEC cards required. *PayPass* cards are ETEC cards subset 6, 8 and Maestro *PayPass*.
3. A terminal Integration Workshop to explain the TIP and the testing that will be performed, to agree on the scope of the TIP, and to confirm the testing configuration.
4. TIP Testing.

## 5.7 ETED

The ETED is designed to validate that all activities under the control of the acquirer (for example, terminal, acceptance network, authorization system, interfaces to MasterCard systems, etc.) function correctly.

It is performed as soon as the implementation is promoted to live.

The acquirer provides MasterCard with the locations of the terminal(s) to be tested. MasterCard uses a representative set of live MasterCard-branded, *PayPass*-approved cards (provided by various issuers) to perform transactions at the terminals to be tested. MasterCard and the acquirer monitor transactions across the real-time authorization network and through the clearing and settlement process. The log files are also verified after the end-to-end tests have been performed.

## 5.8 Post-Live Monitoring

To ensure a smooth rollout and prove that the implementation is stable, MasterCard monitors the acquirer's transactions for a period of 30 days. MasterCard issues the acquirer with a completion notice at the end of this period and the acquirer system is ready to move to business as usual. The acquirer receives confirmation of the successful completion of the period of live monitoring. The acquirer's implementation is now considered as a "Business As Usual" (BAU) system.

## 5.9 Further Information and Contact Details

Queries and further assistance can be obtained from the acquirer's regional representative or the following specific support addresses:

**Table 5.2—Contacts**

Area	Contact
<i>PayPass</i> testing	testing@PayPass.com
General chip help	chip_help@mastercard.com
System buildup testing	chip_help@mastercard.com
TIP	tip@mastercard.com for European projects tip_NA@mastercard.com for North American projects tip_AP@mastercard.com for Asia Pacific projects tip_LAC@mastercard.com for Latin America projects tip_SAMEA@mastercard.com for SAMEA region projects
NIV	Customer Implementation Services (CIS)—Acquirers will be provided the contact details for the Network Interface Testing Engineer assigned to their implementation project.
MEAS (non-U.S. regions)	meas.sim@mastercard.com
MasterINQ debit/credit (U.S. regions)	debit.sim@mastercard.com credit.sim@mastercard.com
Clearing simulator	mcps.sim@mastercard.com
Online software upgrades	www.mastercardonline.com
ETEC cards	chip_help@mastercard.com (for information regarding the use of ETEC cards for pre - testing purposes) test_tools@silicomp.fr (for information regarding the purchase of ETEC cards)

---

# A

## ***PayPass—M/Chip Limit Use – Functional Implementation Examples***

*This appendix illustrates valid implementations of the PayPass—M/Chip Limits.*

---

A.1 Soft Limit Implementations.....	A-1
A.2 Hard Limit Implementations.....	A-4



## A.1 Soft Limit Implementations

Only MasterCard *PayPass*—M/Chip configurations may be soft limit implementations.

The following configurations are shown:

1. MasterCard offline capable terminals.
2. MasterCard online only terminals.

**PayPass—M/Chip Limit Use – Functional Implementation Examples**  
**Soft Limit Implementations**

**Figure A.1— Soft Limit Configuration for MasterCard Offline Capable Terminals**

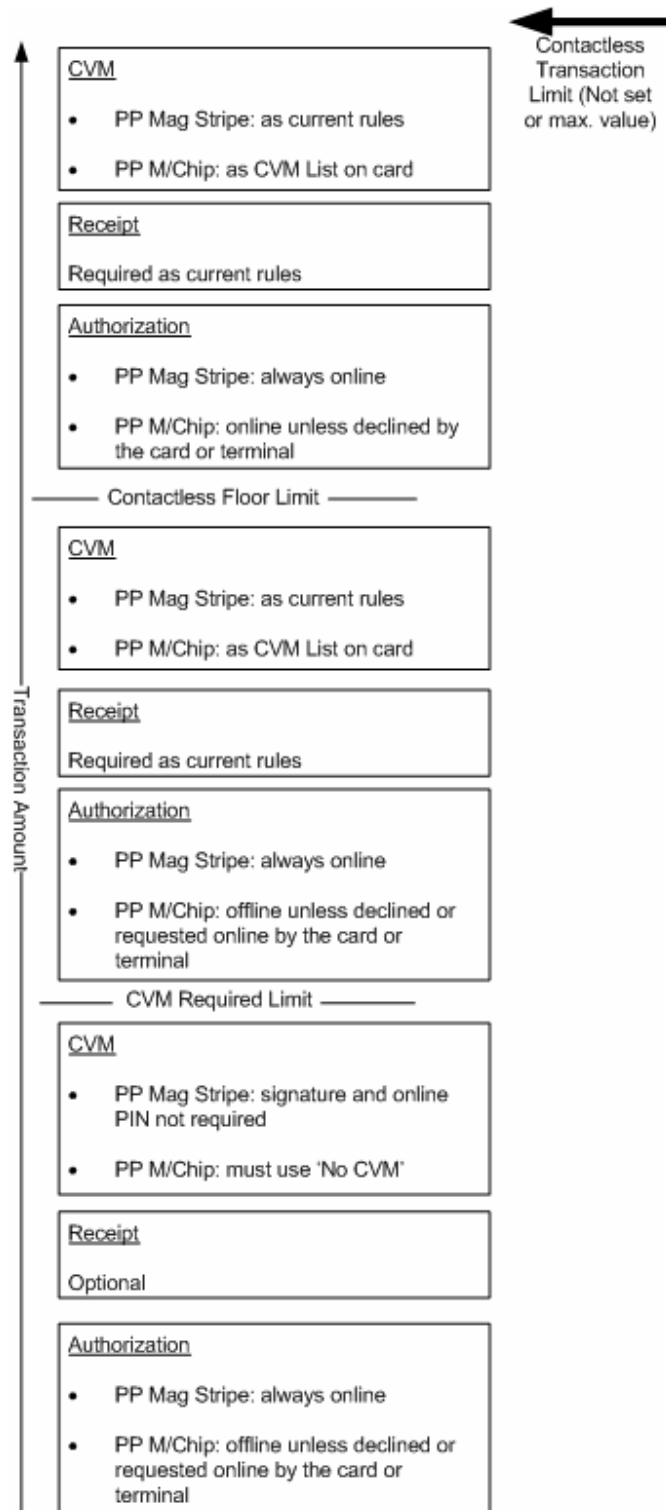
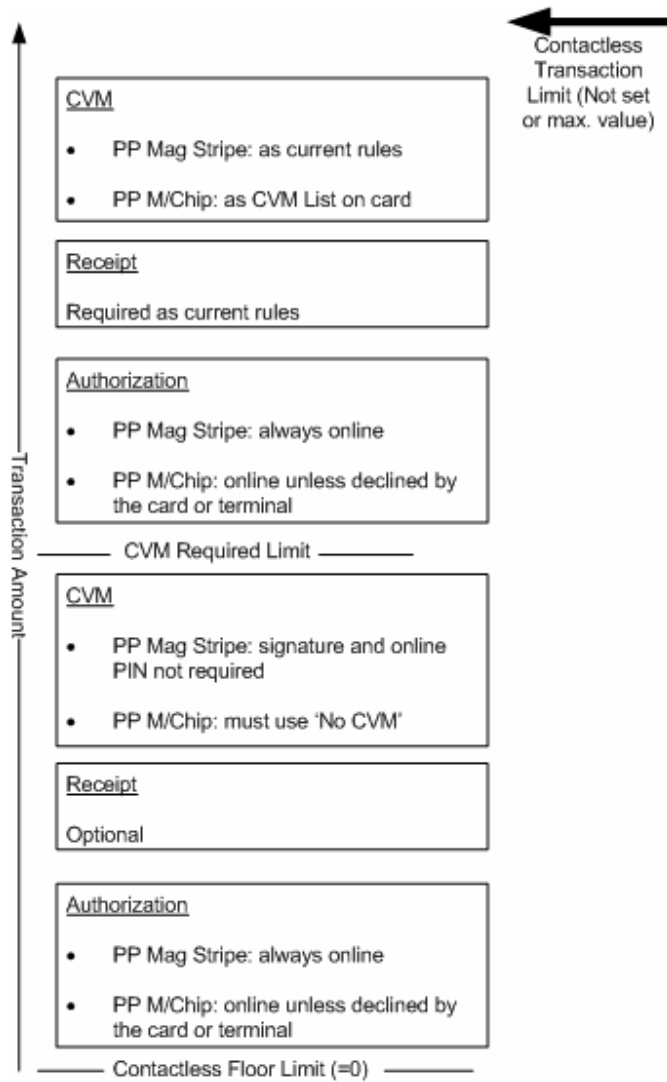


Figure A.2— Soft Limit Configuration for MasterCard Online only Terminals



## A.2 Hard Limit Implementations

Maestro *PayPass* configurations are all hard limit implementations.

MasterCard *PayPass*—M/Chip implementations (with the exception of offline only CAT3 terminals) may hard limit only for a whole region or market. Terminals accepting both Maestro *PayPass* and MasterCard *PayPass*—M/Chip must configure both the Maestro *PayPass* and MasterCard *PayPass*—M/Chip settings.

The following configurations are shown:

1. MasterCard offline capable terminals.
2. MasterCard online only terminals.
3. MasterCard offline only terminals (CAT3).
4. Maestro terminals.

**Figure A.3— Hard Limit Configuration for MasterCard Offline Capable Terminals**

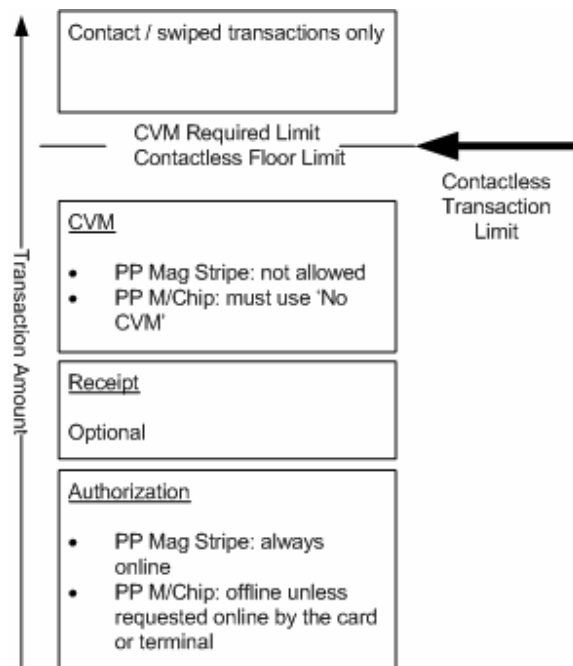
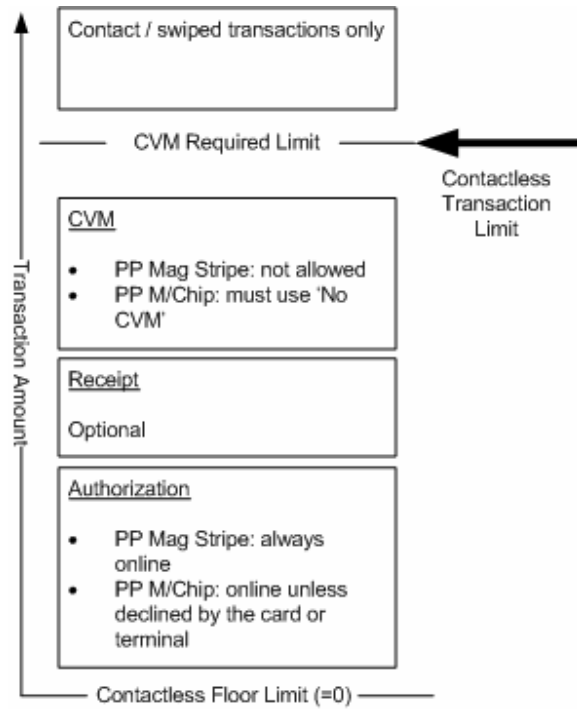


Figure A.4— Hard Limit Configuration for MasterCard Online only Terminals



**PayPass—M/Chip Limit Use – Functional Implementation Examples**  
**Hard Limit Implementations**

---

**Figure A.5— Hard Limit Configuration for MasterCard Offline only Terminals (CAT3)**

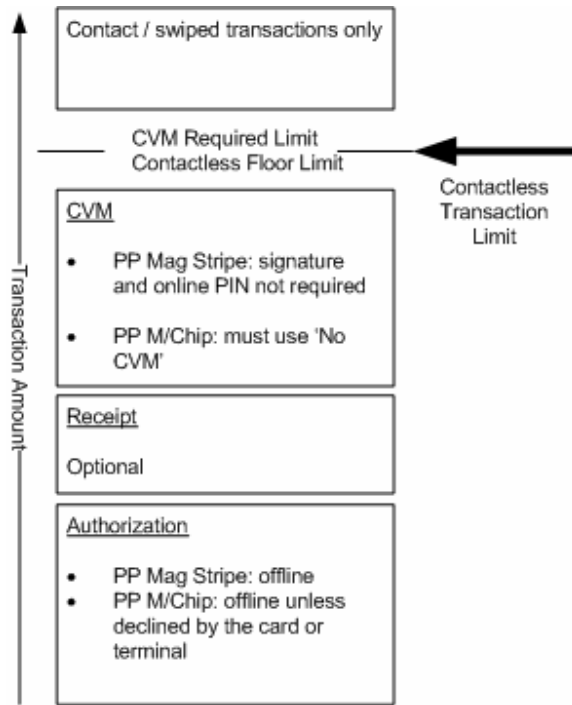
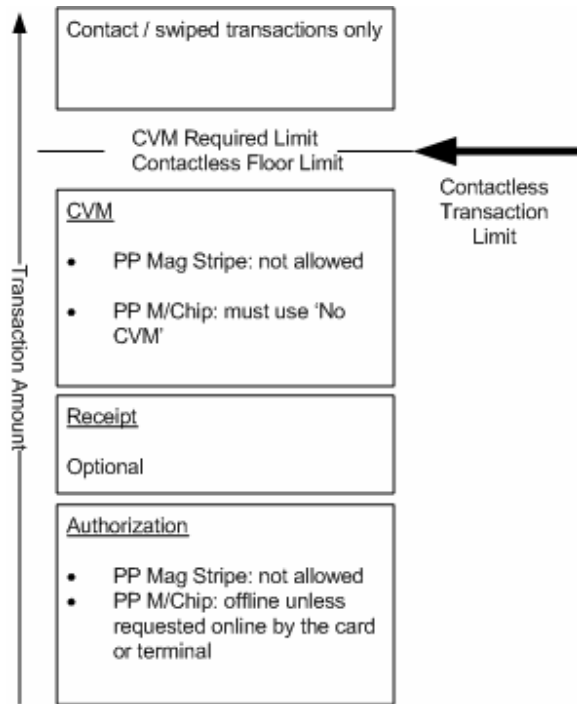


Figure A.6— Hard Limit Configuration for Maestro Terminals





---

# B

## Glossary

*This appendix is a Glossary of Terms used in this document*

---

Glossary of Terms .....	B-1
-------------------------	-----



## Glossary of Terms

Term	Description
M/Chip 4 Application	The M/Chip 4 Select and M/Chip 4 Lite card applications as implemented on issuer's cards and as specified in the MasterCard M/Chip 4 Card Application Specification for Debit and Credit. When behavior is specific to one of the applications, the specific application name (M/Chip 4 Lite application or M/Chip 4 Select application) is used.
Non-Card Form Factor Device	Refer to " <i>PayPass</i> Cardholder Device."
<i>PayPass</i> Approved Terminals	MasterCard tests products for compliance to all required specifications. Products which are proven to comply are issued a <i>PayPass</i> Letter of Approval and are <i>PayPass</i> approved. MasterCard publishes lists of <i>PayPass</i> approved products to help acquirers choose their products. A product may require configuration or further functionality before use, but this must not change the product's compliance with specifications. Approved products are used as part of an overall payment system.
<i>PayPass</i> Cardholder Device	Also referred to as an "NCFE device." A <i>PayPass</i> product allowing cardholders to make contactless <i>PayPass</i> payments, but not in the standard bankcard (ID-1) form. Examples include <i>PayPass</i> tags and key fobs and mobile phones.
<i>PayPass</i> —M/Chip Application	The M/Chip 4 card application, extended for communication over a contact and contactless interface as specified in the MasterCard <i>PayPass</i> —M/Chip Technical Specification manual.
<i>PayPass</i> —M/Chip Card	Dual-interface card with the <i>PayPass</i> —M/Chip Application accessible over the contact and contactless interface.
<i>PayPass</i> —M/Chip Terminal	A terminal accepting <i>PayPass</i> —M/Chip cards using a transaction flow similar to the EMV contact transaction flow and supporting Terminal Risk Management (TRM). If the terminal has offline capability then it will also support offline CAM. The terminal may also accept existing magnetic stripe cards and contact cards. The <i>PayPass</i> —M/Chip terminal must also accept <i>PayPass</i> —Mag Stripe transactions. It may also accept other contactless schemes.

## Glossary

### Glossary of Terms

---

<b>Term</b>	<b>Description</b>
<i>PayPass—M/Chip Transaction</i>	A <i>PayPass</i> transaction which includes the required M/Chip EMV data elements as used in Authorizations and Clearing messages.
<i>PayPass—Mag Stripe Transaction</i>	A <i>Paypass</i> transaction which contains the required mag stripe only data elements.
<i>Paypass Technology</i>	The MasterCard specific implementation of ISO/IEC 14443. <i>Paypass</i> uses the technology as defined in the <i>Paypass—ISO/IEC 14443 Implementation Specification</i> for the wireless (“contactless”) exchange of data between card and terminal.
<i>Paypass Terminal Vendor Testing</i>	The MasterCard process of testing products for compliance to all required specifications. Products which pass all the required tests are <i>Paypass</i> -approved products.
<i>Paypass Transaction</i>	A payment transaction using <i>Paypass</i> technology for the data exchange between card and terminal. A transaction can be either a <i>Paypass—M/Chip Transaction</i> or <i>Paypass—Mag Stripe Transaction</i> .
<i>Paypass Transaction Time</i>	The time the <i>Paypass</i> card needs to be present in the terminal’s electromagnetic field in order to allow for a complete data exchange. The completion of the data exchange is indicated by a beep and a visual indication. Any processing done by the terminal after the card has been removed is excluded from the <i>Paypass</i> transaction time.