MasterCard International

MasterCard® *PayPass*™

Mag Stripe, Acquirer Implementation Requirements

TABLE OF CONTENTS

1. PURPOSE OF THESE REQUIREMENTS

The purpose of this document is to help MasterCard acquirers implement MasterCard's *PayPass* program. *PayPass* enables consumers to either tap their *PayPass* card or device on *PayPass*-enabled terminals or use the *PayPass* card's traditional magnetic stripe at all other MasterCard locations. These requirements will:

- Help acquirers to understand, implement, and support *PayPass* card or device acceptance.
- Explain the differences between *PayPass* cards or devices and traditional magnetic stripe cards.
- Help plan and implement a successful project to realize these benefits.

1.1 Scope of These Requirements

These requirements are limited to the implementation of MasterCard *PayPass*—Mag Stripe. This is the version of *PayPass* intended for use where transactions are predominantly authorized online, such as in North America. It does not describe how to implement other MasterCard chip applications or M/Chip functions. It describes the incremental changes required to enable merchants' point-of-sale (POS) systems to accept *PayPass* transactions. These requirements should be used during the implementation phase of enabling *PayPass* processing, after the decision to support MasterCard *PayPass* transactions has been made.

For those acquirers that provide equipment and support to merchants, detailed requirements for merchant implementation can be found in the *MasterCard PayPass Merchant Implementation Requirements*.

1.2 Effect of These Requirements

These requirements are intended to provide general guidance to help MasterCard acquirers accept *PayPass* contactless transactions. The responsibility for the content and execution of any implementation will remain with the acquirer.

To the extent permitted by law, neither MasterCard International nor any of its affiliates, employees, or offices shall be liable to any recipient of these requirements, or any other third party for any loss, damages (including direct, special, punitive, exemplary, incidental, or consequential damages), or costs (including attorneys' fees) which arise out of, or are related to, these requirements. The foregoing limitation of liability shall apply to any claim or cause of action under law or equity whatsoever, including contract, warranty, strict liability, or negligence, even if MasterCard has been notified of the possibility of such damages or claim.

Where these requirements refer to the availability of services and/or documentation from MasterCard, the terms on which such services or documentation are made available shall be specified by MasterCard as and when such services or documentation are requested.

These requirements must be kept strictly confidential and must not be disclosed to any third party save to such of your employees as are required to have access to the same in the performance of their duties. Save as above, these requirements may not be duplicated, published, or disclosed in whole or part without the written permission of MasterCard International Incorporated.

1.3 Guidance on Terminology

Due to the legacy of the plastic card industry and the fact that the first *PayPass*-compliant form factor is card based, the term "card" is used frequently throughout. However, the contactless nature of *PayPass* permits non-card form factors. These are referred to as *PayPass* devices.

The functionality of both *PayPass* cards and devices is driven by the chip inside and is independent of the form factor in which the chip resides, therefore the default reference for the consumer token in this document is either "*PayPass* card" or "*PayPass* card or device." Where there are specific requirements or considerations resulting from the form factor, then this will be clear from the use of the reference "device."

All other terms are detailed in Appendix B, *Glossary*.

2. MASTERCARD *PAYPASS* OVERVIEW

2.1 What Is MasterCard *PayPass*?

PayPass is MasterCard International's proximity payments program. It allows consumers to make MasterCard payments without having to hand over or swipe a payment card. To make a payment, the consumer simply taps their *PayPass* card or device on to a *PayPass* reader. The details are read from the card or device using the contactless interface, and an enhanced payment transaction is then performed over the standard magnetic stripe network infrastructure. *PayPass* is ideal for those environments where speed and convenience are valued; for example, fuel pumps, quick-service restaurants (QSRs), drive-thrus, convenience stores, vending machines, and toll booths.

MasterCard *PayPass* cards look similar to standard MasterCard cards, except that they include the *PayPass* identifier on the front and a shorter signature panel, as used for chip cards, on the back. However, in addition to a magnetic stripe on the back, embedded inside the card there is a contactless chip that stores and processes the payment account data and a connected antenna that typically runs around the perimeter of the card as shown in Figure 1a or, in some circumstances where fourth-line embossing is required, in a reduced configuration (Figure 1b).

Figure 1a, MasterCard *PayPass* Card with Full Antenna Configuration

Figure 1b, MasterCard *PayPass* Card with Reduced Antenna Configuration

PayPass devices are available in a variety of forms, from the traditional card introduced above to smaller-sized 2D and 3D key fobs. In fact, *PayPass* devices have the potential to be a wide range of shapes and sizes. The design choice resides with the financial institution issuing the device to the consumer.

While the external shape and size can vary, the internal workings of all *PayPass* devices are similar. Each device contains a chip that stores and processes account data along with an antenna that is used to transmit data through the air to the *PayPass* reader, and from the reader to the card or device. The antenna is connected to the chip and, typically, runs near the inside perimeter of the card or device.

PayPass devices (2D and 3D fobs) typically make use of the same chip and application software as *PayPass* cards, but with the chip and antenna contained in a different housing. *PayPass* devices conduct MasterCard *PayPass* transactions in the same way as *PayPass* cards. To make a payment, a *PayPass* device is tapped on a *PayPass* reader in the same way a *PayPass* card would be. *PayPass* readers do not need to be changed to accept *PayPass* device-initiated transactions.

Examples of two potential *PayPass* device designs, a 2D fob and 3D fob, are illustrated below:

Figure 2, MasterCard *PayPass* 2D Fob

Figure 3, MasterCard *PayPass* 3D Fob

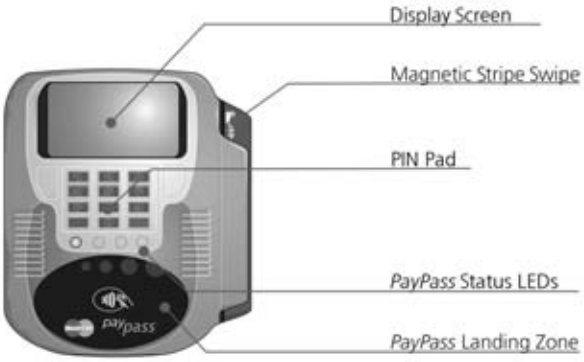
2. MASTERCARD *PAYPASS* OVERVIEW

MasterCard *PayPass* consumers simply tap their card or device on the *PayPass* reader (read starts typically within 1.5 inches or 4 cm). The *PayPass* "landing zone," where consumers should tap their card or device, is clearly indicated by the *PayPass* landing zone identifier, an example of which is shown in Figure 7.

Figure 4, MasterCard *PayPass* Device Presentation

MasterCard *PayPass* readers include an antenna and connected electronics that allow a *PayPass* card or device to be read. These readers may be integrated within a payment terminal or stand alone. MasterCard *PayPass*–capable POS terminals therefore may support acceptance of both traditional magnetic stripe and *PayPass*, or *PayPass*-only transactions. Examples of both types are shown below.

Combined Magnetic Stripe Terminal and *PayPass* Reader
(with PIN pad and electronic signature capture display)



Used to provide *PayPass* and magnetic stripe acceptance at POS

***PayPass*-only Reader**

Used to provide *PayPass*-only acceptance at POS

Figure 5, MasterCard *PayPass* POS Equipment

Once the data has been read by the *PayPass* reader, the payment transaction data is passed through the merchant's POS system and is processed through the payment systems network used for existing card-based transactions.

The MasterCard *PayPass* program includes the following:

- Detailed specifications for all aspects of the program
- Type approval services for vendor products (cards, terminals, and devices) to ensure compliance with the specifications and interoperability
- Marketing and promotional materials and advertising
- Consumer marketing materials for issuers
- Merchant POS materials
- Business and technical support to MasterCard issuers, acquirers, and merchants deploying *PayPass*

2.2 How Is MasterCard *PayPass* Used?

2.2.1 The Payment Process

A typical *PayPass* transaction sequence is shown below.

Figure 6, Typical MasterCard *PayPass* Transaction

Step 1—*PayPass* terminal/reader in the ready state waiting for consumer to present card or device. A single indicator light shows the ready state.

Step 2—Consumer taps card or device on landing zone and terminal reads data. Once completed, visual and audible cues are provided.

Step 3—Consumer removes card or device. The visual indicators go off and the transaction is processed in the normal way by the merchant.

All *PayPass* terminals must identify where a customer must tap their *PayPass* card or device to achieve a successful read; this identified area is referred to as the "landing zone."

Figure 7, Example of a MasterCard *PayPass* Landing Zone Identifier

The landing zone must be a clearly distinguishable area on the terminal. To ensure a consistent approach of identifying the landing zone, the contactless symbol must be placed in the center of the landing zone in a position on the terminal that indicates the strongest part of the radio frequency signal that the terminal generates, referred to as the "operating volume," to read the *PayPass* card or device.

If space permits, MasterCard *PayPass* and other scheme branding may also be placed on the landing zone as long as branding rules are maintained and the contactless symbol is not obscured in any way and continues to indicate the center of the landing zone. If space on the landing zone does not permit scheme branding to be included, then this should be placed in such a way as not to detract the customer from identifying the contactless symbol and the landing zone.

MasterCard *PayPass* terminal product approval uses the contactless symbol during testing to identify the landing zone and test that the center of the contactless symbol is positioned directly over the strongest part of the operating volume.

2.2.2 Where Can MasterCard *PayPass* Be Used?

The MasterCard *PayPass* contactless functionality can be used at any merchant location that has installed *PayPass* terminals. The merchant segments where *PayPass* is expected to be most attractive include:

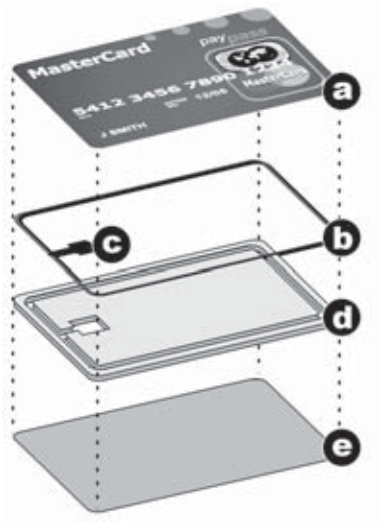
- QSRs/Fast Food Restaurants (MCC 5814)
- Movie Theaters (MCC 7832)
- Parking Lots (MCC 7523)
- Convenience Stores/Vending Machines (MCC 5499)
- Drug Stores/Pharmacies (MCC 5912)
- Gas Stations/Petroleum (pay-at-the-pump and in-store) (MCC 5541)
- Video Rental Stores (MCC 7841)
- Bookstores (MCC 5942)
- Music Stores (MCC 5735)
- Newsstands (MCC 5994)
- Grocery Stores/Supermarkets (MCC 5411)
- Dry Cleaners (MCC 7216)

2.3 How MasterCard *PayPass* Works

2.3.1 MasterCard *PayPass* Cards and Devices

PayPass cards and devices all consist, at the basic level, of an antenna connected to a chip in a module (b and c in Figure 8 below). These components are typically encapsulated into "carriers" of different shapes and sizes.

For a MasterCard *PayPass* card, the components are contained in a card-sized sheet of plastic, known as an inlay (b, c, and d). This inlay is sandwiched between front and back plastic sheets (a and e) to form a finished card.



(a) Card Front

(b) Antenna

(c) Chip Module/Package

(d) Inlay

(e) Card Back

Figure 8, MasterCard *PayPass* Card Construction

The *PayPass* chip is encoded with data and contains cryptographic data used to authenticate the card or device to the issuer.

PayPass chips are both powered by and communicate using radio frequency (RF) energy provided by the *PayPass* reader. In simple terms, the reader makes energy available to the chip by inducing an electromagnetic field into the air close to the reader. When the chip is moved into this field, electrical energy is provided to it via the antenna (a coil of wire). This energy is used to power the chip; the *PayPass* card or device does not need a battery.

In addition to powering the chip, the reader communicates information to it by changing the amount of energy sent. The chip detects the changes and captures messages from the reader. The chip is also able to send messages to the reader by changing the amount of energy that it uses. The reader detects the change in energy and uses this to understand messages sent back to it.

The contactless nature of the chip and reader interaction allows the form factor that contains the *PayPass* chip and antenna to vary in shape and size, since they do not need to be physically inserted or slid through a reader.

MasterCard *PayPass* cards are the traditional bankcard size and shape as defined by ISO 7810.

MasterCard *PayPass* devices, however, can be created in a variety of forms depending on issuer requirements and consumer needs. For example, a small device may be created that can be attached to a key ring, which, as it is easily carried, may increase convenience for the consumer. Although *PayPass* devices do not look like *PayPass* cards, their internal workings may be the same. They typically contain the same chip, the same application software, and a radio antenna. As the antenna usually runs around the edge of the device, it is likely that the internal layout of components will be different for each device design.

The use of a MasterCard *PayPass* device is permitted only as a companion device to a MasterCard card.

From a consumer's point of view the most significant difference between *PayPass* cards and devices is their physical appearance. MasterCard has not imposed constraints on the physical size and shape of *PayPass* devices and, providing the device complies as required with all MasterCard branding, rules, and approval requirements, issuers are able to use any design form factors.

The following diagram illustrates an example of a *PayPass* 2D fob that could be manufactured and personalized in the same way as a *PayPass* card. A small signature panel is provided with room for an external unique identifier.

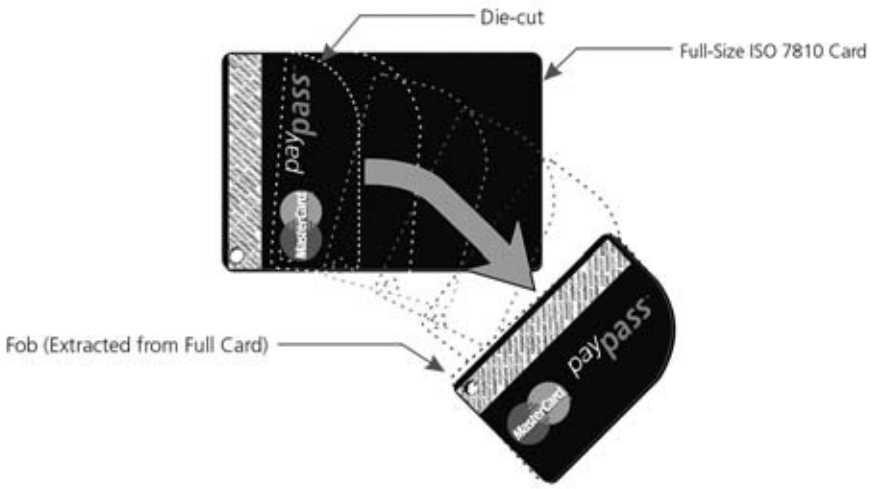
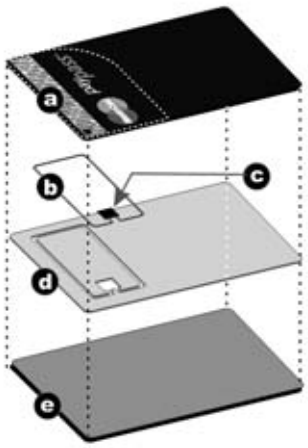


Figure 9, MasterCard *PayPass* 2D Fob

In common with a full-sized card, the *PayPass* 2D fob contains all the elements needed for *PayPass* proximity payments. The difference is that the antenna is smaller. This is illustrated in Figure 10.



(a) Fob Back Containing Signature Panel (optional)

(b) Antenna

(c) *PayPass* Chip

(d) Inlay

(e) Fob Front

Figure 10, MasterCard *PayPass* 2D Fob Construction

An example of a *PayPass* 3D fob that attaches to a key ring is illustrated in the diagram below.

Figure 11, MasterCard *PayPass* 3D Fob

As with a standard MasterCard *PayPass* card, the *PayPass* 3D fob contains all the elements needed for *PayPass* transactions, with antenna design such that the minimum requirements for range can be met.

It is also possible for *PayPass* chips to be embedded into consumer devices, such as a watch or a cell phone, either during manufacture or after purchase. In these circumstances, the consumer device may well have a pre-existing antenna (e.g., a cell phone).

2.3.2 MasterCard *PayPass* Terminals

Information communicated by the *PayPass* chip is taken by a *PayPass* reader, formatted appropriately, and then processed through the merchant's existing POS systems for authorization, clearing, and settlement.

All MasterCard *PayPass* terminals utilize a common user interface to provide a consistent consumer and merchant experience. This ensures that consumers and merchants always know what to expect at the POS when using *PayPass*. This is a key element in making *PayPass "The Simpler Way to Pay™."* Audiovisual cues are used to guide consumers through a *PayPass* transaction, as follows:

1) Ready State

The *PayPass* terminal is in the ready state when a single indicator light shows. This indicates that the *PayPass* reader is ready to accept a *PayPass* card or device.

2) Reading

The *PayPass* reader detects that a MasterCard *PayPass* card or device is present and reads the data required for processing the transaction.

PayPass reading range is typically 1.5 inches (4 cm).

3) Completion State

Once the *PayPass* card or device has been read (this typically takes 0.2 seconds), the terminal will display a sequence of visual indicators, and a sound cue, usually a number of beeps, is heard. Once all visual indicators are lit, they will stay on for approximately 0.3 seconds, during which the sound cue can also be heard. This indicates that the consumer can remove the *PayPass* card or device.

4) Final End State or Error

Soon after the *PayPass* chip is read, the terminal returns to the ready state, waiting for the appearance of a new *PayPass* card or device.

In some cases, the *PayPass* reader may fail to read the card or device (e.g., if it is not *PayPass* capable or if more than one *PayPass* card or device is detected). In this case, neither visual nor audible cues will operate and the *PayPass* terminal will remain in the ready state.

Figure 12, Typical MasterCard *PayPass* Terminal Audiovisual Sequence

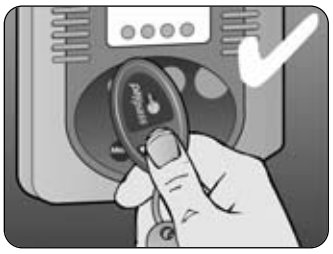
While the reader indicates a successful read using visual and audible cues, it is important to remember that a successful read is only the first step in a payment transaction.

The *PayPass* visual and audible cues do not indicate that the transaction has been authorized, just that the *PayPass* read process is complete and the consumer can remove their card or device from the reader. The authorization is indicated by the POS equipment in the same manner as for all MasterCard-based transactions.

2.3.3 How to Tap *PayPass* Cards and Devices

In order for *PayPass* cards and devices to be read, they must be presented to the *PayPass* terminal in the correct manner as shown in Figure 13 (a and b) below. This is where the card or device is in the center of the landing zone and is close to being flat against the universal contactless symbol shown in Figure 13(c).

a) Correct "almost-flat" presentation for *PayPass* card



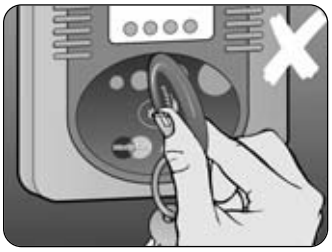
b) Correct presentation (keys and other contactless devices held away from the terminal) for *PayPass* fob

c) Universal contactless symbol

Figure 13, Correct Presentations of *PayPass* Cards and Devices

Presenting a *PayPass* card or device on edge to the landing zone (Figure 14 [a and b]), as if cutting it with a knife, or with other *PayPass* cards or devices or other non-*PayPass* contactless cards or devices at the same time (Figure 14[c]) is incorrect; only the *PayPass* card or device to be used should be presented.

a) Incorrect "on-edge" card presentation



b) Incorrect "on-edge" device presentation

c) Incorrect presentation: only the *PayPass* card or device to be used should be presented, e.g., a wallet/purse with multiple cards should not be presented.

Figure 14, Incorrect Presentations of *PayPass* Cards and Devices

If a *PayPass* card or device is attached to a bunch of keys, other metallic objects, or other contactless devices as shown in Figure 15, these should all be kept away from the terminal, typically in the palm of the user's hand. If keys or other contactless devices are presented to the *PayPass* terminal they may interfere with the reading of the device being presented.

Incorrect presentation: other metallic objects or other contactless devices should all be kept away from the terminal, typically in the palm of the user's hand.

Figure 15, Incorrect Presentation of Other Object or Contactless Device

The likelihood of a terminal read error will be greatly diminished if the guidelines above are followed.

2.3.4 Ensuring MasterCard *PayPass* Interoperability

PayPass cards, devices, readers, and terminals are manufactured by multiple vendors. To ensure that all *PayPass* cards and devices work with all *PayPass* readers, MasterCard provides detailed specifications and requires vendors to submit products for type approval testing before deploying these into the marketplace.

The MasterCard *PayPass* specifications are based on international standards for contactless chip cards, namely the ISO/IEC 14443 standard. The detailed MasterCard *PayPass* specifications, available to licensees, can be obtained by sending an e-mail request to specifications@paypass.com.

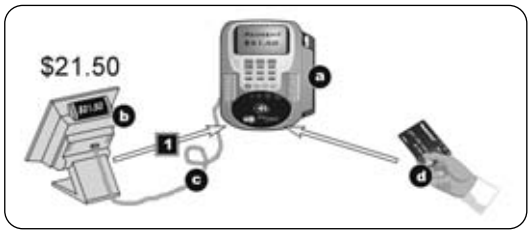
2.4 Processing MasterCard *PayPass* Transactions

2.4.1 Process Description

Once a card or device has been read, the authorization message is transmitted to the acquirer in the same way as a traditional magnetic stripe transaction. While no new data protocols are necessary, it is important to note the following aspects of MasterCard *PayPass* transaction processing:

- **Transaction Authorization and Clearing**—These process flows are the same as for magnetic stripe transactions or M/Chip transactions.
- **Transaction Coding**—*PayPass* is designed to have minimal impact on merchants' and acquirers' existing systems. Merchants do, however, need to ensure that their acquirer has up-to-date information on *PayPass* terminal capability, that *PayPass* transactions are coded correctly, and that the acquirer has completed end-to-end testing with MasterCard CIS to ensure data element compliance with credit, signature debit, and PIN debit transactions. (More detail on transaction coding is provided in Section 2.4.2, *Transaction Coding*.)
- **Existing Payment Program Rules**—*PayPass* improves the process for reading the payment account data and can be used with different payment products. However, it is important to remember that the rules applying to these underlying payment programs must still be observed. Therefore, if the underlying payment program requires that the consumer sign a receipt or enter a PIN, then all participants in the payment process must comply with these requirements.

A typical *PayPass* transaction is shown in the sequence below:

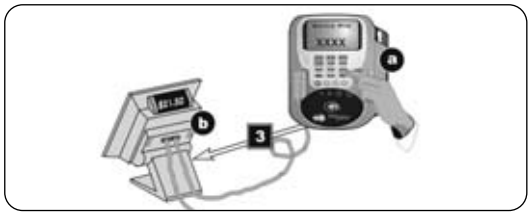


1 Transaction amount sent to *PayPass*-enabled consumer-facing terminal (CFT) ⓐ from the electronic cash register (ECR) ⓑ. The CFT ⓐ is connected to the ECR via a cable ⓒ so that dual amount entry is not required.

2i Consumer presents device to CFT.

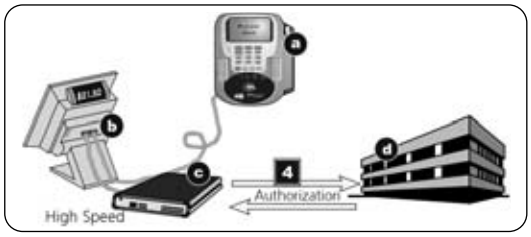
2ii *PayPass* reader reads data from the *PayPass* device in 0.2 seconds.

2iii *PayPass* device is removed.

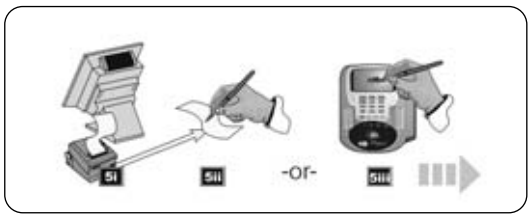


3 If required, consumer enters PIN for online verification.

This is submitted as part of the online authorization process detailed next.



4 Online authorization of the transaction is obtained (via high-speed connection such as a DSL modem) from the payment acquirer ⓓ.



5 When required, a receipt is printed **5i** and a consumer signature is physically **5ii** or electronically captured **5iii**.

Figure 16, Typical MasterCard *PayPass* Transaction Including Authorization

REQUIREMENT

MasterCard *PayPass* transactions must be processed online to realize full risk management capabilities.

MasterCard *PayPass* transactions are passed from the merchant to the payment account issuer via the merchant acquirer in the normal way, consistent with the rules for the underlying payment program.

The only difference is that the transaction is coded to indicate a *PayPass*-read transaction using the correct POS entry mode and Terminal Data Input Capability values in the relevant data elements within the various MasterCard network messages. These values are used by the MasterCard payment account issuer to identify and differentiate *PayPass*-read transactions from magnetic stripe–read transactions and to allow appropriate risk management decisions to be made.

2.4.2 Transaction Coding

It is important from a risk management and information management perspective that MasterCard *PayPass* transactions and *PayPass* terminal capability can be identified from transaction data.

Issuers, acquirers, merchants, and MasterCard require information on the entry mode for each transaction and the POS terminal capability to:

- Identify and prevent fraud at the merchant.
- Monitor usage of cards, devices, and terminals.
- Track terminal *PayPass* capability.
- Measure return on investment in enabling cards or devices and POS terminals.
- Manage chargeback processing.

To facilitate the above, the POS system must include new values in certain existing data elements in the authorization and clearing records.

- The appropriate Banknet and GCMS messages must be populated with the corresponding POS entry mode.
- It is also important to indicate whether the POS is *PayPass*-enabled or not (regardless of how a transaction is initiated).

REQUIREMENT

Correct coding and processing of MasterCard *PayPass* transactions and terminal capability are mandatory for all *PayPass* authorization and clearing messages.

2.4.3 POS Entry Mode/POS Terminal Data Input Capability

Merchant POS systems must provide the information needed by acquirers to populate data elements that indicate a *PayPass* transaction.

Merchants must ensure that:

- POS equipment communicates the POS entry mode (contactless, swiped, or keyed) to their acquirer.

Acquirers must ensure that:

- Merchants are fully aware of the capabilities of each terminal, particularly those that are enabled to accept *PayPass* cards or devices.
- They correctly code and pass the Banknet and GCMS messages to indicate the correct POS entry mode (contactless, swiped, or keyed).
- They correctly code transactions to indicate that a terminal is able to accept *PayPass* cards or devices. This is normally done by the acquirer managing a list of terminal capabilities against the terminal identification number.

***PayPass* issuers must ensure that:**

- Their systems can correctly receive and process the messages containing the POS entry mode (DE 22) and POS Terminal Device Data Input Capability (DE 61) data elements and make appropriate authorization decisions.

More Information

Details of the above requirements can be found in Section 6 of the *MasterCard PayPass Product Guide* (available by sending an e-mail to specifications@paypass.com) and in the appendices of these requirements as noted:

- Appendix A, "Data Element Values for MasterCard *PayPass*," Global Operations Bulletin No. 6, 1 June 2005, pp. 60–65

2.4.4 Signature and Chargeback Requirements

The rules governing *PayPass*-read payment transactions are dictated by the rules of the payment product (credit, debit, etc.) referenced by the account number on the *PayPass* card or device, and the rules governing acceptance in the merchant location where the transaction occurs.

While the fundamentals of a transaction remain the same, the physical characteristics of *PayPass* devices may introduce some differences in the overall payment process—for example, when making a purchase, a *PayPass* card or device remains in the possession of the consumer throughout the transaction, and the device itself may not have a signature panel, making signature verification challenging. These variations have been accommodated by changes to the rules governing the underlying payment product.

A signature is not required and a receipt is optional for a transaction equal to or less than the equivalent of US $25 undertaken using a *PayPass* card or device. PIN may be required for debit.

A properly identified *PayPass* transaction (magnetic stripe-read or M/Chip-read), equal to or less than the equivalent of US $25, is protected against chargebacks under the following reason codes:

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

NOTE

For Quick Payment Service (QPS) registered merchants who accept *PayPass*, the QPS program supersedes the *PayPass* rules. For more information on the QPS program, please refer to the *QPS Manual*.

2.4.5 Refunds

The processes associated with MasterCard *PayPass* transactions are identical to those for traditional magnetic stripe card–read transactions. Therefore, if a consumer is entitled to a refund or if a transaction needs to be voided, existing processes apply.

One of the requirements for refunds is that the originating card or device be used at the time of the refund. This requirement is unchanged; the *PayPass* card or device should be used to process refunds. Merchants must ensure that the consumer refund service area is suitably equipped with *PayPass* terminals.

3. TYPICAL MASTERCARD *PAYPASS* MERCHANT INSTALLATION

3.1 Overview

MasterCard *PayPass* has been designed to limit the impact on existing acceptance processes and equipment as far as possible. However, to achieve the desired benefits of using the *PayPass* technology, the merchant should consider a number of factors in how to implement it. This section outlines a typical merchant installation as an illustration of the key hardware components that will be needed, and then discusses key aspects of the payment transaction that may require different processing from what might have been implemented for traditional magnetic stripe–read transactions.

In reading the following subsections, it should be remembered that *PayPass* is basically an alternative to magnetic stripe read in transferring payment account details from consumer to merchant. All the underlying payment account acceptance rules remain unchanged.

This means that the merchant should expect to see all of MasterCard's payment programs using *PayPass* technology and will need to follow the program rules pertaining to these programs in processing *PayPass* transactions.

3.2 POS Equipment

A typical merchant installation involves integrating a MasterCard *PayPass*–capable terminal into the POS environment, as shown below:

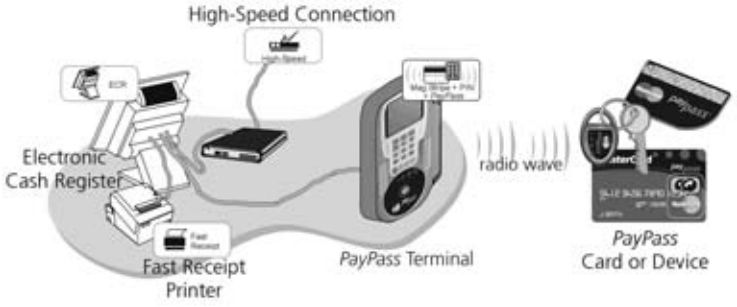


Figure 17, A Typical MasterCard *PayPass*–Enabled POS

PayPass Terminal

For merchants that currently accept payment cards, implementing *PayPass* involves adding *PayPass* terminals or readers to existing POS equipment, such as ECRs and magnetic stripe terminals. Merchants may consider replacing existing POS terminals with new ones that have integrated *PayPass* support, or installing new POS equipment configured to support *PayPass*.

For merchants that do not currently accept payment cards, implementing *PayPass* involves installing new *PayPass*-enabled POS equipment.

MasterCard recommends use of POS terminals with integrated *PayPass* support.

Connecting a *PayPass* reader to an existing magnetic stripe terminal using any form of dynamic magnetic stripe or magnetic induction coupling to the existing magnetic strip reader is not permitted by MasterCard.

High-Speed Connection

The benefits of MasterCard *PayPass* are maximized when used with high-speed authorization lines such as DSL, V-SAT, leased lines, cable modems, and other high-speed connections. As such, *PayPass* merchant telecom lines must support a transaction (authorization) time of less than 4 seconds.

ECR

If the merchant is using a separate ECR and POS terminal, then connecting these is required. This integration eliminates the need for dual-amount entry by the clerk and is a key time-saver in the *PayPass* transaction process.

Fast Receipt Printer

While no changes to the ECR may be required, a high-speed receipt printer is highly recommended, one that typically prints a receipt in less than 2 seconds; a key advantage of *PayPass* lies in speed and convenience, and a slow receipt printer adds to the overall transaction time.

REQUIREMENTS

- The automatic communication of the purchase amount to the POS terminal is required. This eliminates the need for dual entry.
- High-speed authorization connections (e.g., broadband or DSL) are required to ensure merchants and consumers realize the optimal speed benefits of *PayPass* at the POS. *PayPass* merchant telecom lines should support an authorization time of less than 4 seconds.
- Separate *PayPass* readers/coupling devices must have a physical cable connection to any existing POS terminal. Magnetic induction coupling is not permitted.

RECOMMENDATION

The use of high-speed receipt printers is highly recommended; a key advantage of *PayPass* lies in its speed and convenience and a slow receipt printer adds to the overall transaction time for the merchant and consumer.

3.3 Transaction Processing

3.3.1 Extended Service Code

MasterCard *PayPass* card or device issuers may choose to use extended service code values in the *PayPass* chip different from those typically used for magnetic stripe cards. For this reason acquirers must ensure that:

- Their processing systems support extended service codes.
- All merchant POS solutions allow the use of extended service codes.

Test cards or devices provided by MasterCard will check that cards or devices with specific extended service codes are processed correctly, but it is the merchant's and acquirer's responsibility to ensure full compliance with this requirement in accordance with MasterCard rules.

3.3.2 Track 1 and 2 Data Integrity

Some existing POS systems collect Track 1 data, truncate it, and process it as Track 2; however, *PayPass* Track 1 and 2 data may be different.

For this reason, merchants and acquirers must make sure that Track 1 data is processed as Track 1 and Track 2 data is processed as Track 2. If data from one track is presented as the other, this may cause the transaction to be rejected by the consumer's card issuer.

3.3.3 Chargebacks

PayPass provides a new, faster, and more convenient entry mechanism for account details than that offered by traditional cards. Although the entry mode is new, transaction liability remains the same as for the underlying payment account when the payment is made with a magnetic stripe.

A properly identified *PayPass* transaction (magnetic stripe-read or M/Chip-read), equal to or less than the equivalent of US $25, is protected against chargebacks under the following reason codes:

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

NOTE

For QPS registered merchants who accept *PayPass*, the QPS program supersedes the *PayPass* rules. For more information on the QPS program, please refer to the *QPS Manual*.

3.3.4 Checking Signatures

While the fundamentals of a transaction remain the same, the physical characteristics of *PayPass* devices may introduce some differences in the overall payment process—for example, when making a purchase, a *PayPass* card or device remains in the possession of the consumer throughout the transaction, and the device itself may not have a signature panel, making signature verification challenging. These variations have been accommodated by changes to the rules governing the underlying payment product.

A signature is not required and a receipt is optional for a transaction equal to or less than the equivalent of US $25 undertaken using a *PayPass* card or device. PIN may be required for debit.

If the consumer disputes a transaction needing a signature, the merchant is required to provide evidence that the accountholder performed the transaction. This requires that the merchant obtain a signature at the time of the transaction.

MasterCard recommends that merchants retain evidence of consumer signatures in the normal way for all transactions that require them.

3.3.5 Refunds and Voids

The processes associated with payments are the same for MasterCard *PayPass* transactions as they are for traditional card transactions. Therefore, if a consumer is entitled to a refund or if a transaction needs to be voided, existing processes apply.

One of the requirements for refunds is that the originating card be used at the time of the refund. This is the same for *PayPass* cards and devices. The *PayPass* card or device should be used to process refunds. Merchants must ensure that the refund consumer service area is suitably equipped with *PayPass* terminals.

3.3.6 Failed Reads

As described in Section 2.3.2, at the end of a *PayPass* card or device read process, the MasterCard *PayPass* reader returns to the ready state approximately one second after a *PayPass* card or device has been read. In this state, the reader is waiting for the introduction of a new card or device.

There are some instances when the reader may fail to read the card or device correctly. In these cases, the green lights do not light, the beep does not sound, and the reader remains in the ready state.

A failed read can occur when:

- The consumer taps a card or device on the reader that is not *PayPass* enabled.
- The consumer taps more than one *PayPass* card or device on the reader at the same time.

It is important to note that reading the *PayPass* card or device is the first step in a transaction, and that a green light and a beep do not indicate an authorized transaction. If appropriate, consumer verification (signature/PIN) still has to be obtained by the merchant, the transaction still has to be submitted for authorization, and a response (either accept or decline) returned by the issuer.

3.3.7 Device Retention

For traditional magnetic stripe cards that tend to be handed to the merchant to swipe, authorization messages returned by the issuer can instruct merchants to retain the consumer's card when there is a problem with the account. MasterCard *PayPass* cards and devices operate under the same rules for accounts as existing cards, which means authorization messages for issuers will still occur.

Since the consumer remains in control of the *PayPass* card or device throughout the transaction, the opportunity for merchants to "pick up" or "capture" these cards or devices will be limited. Issuers are aware that the chances of a *PayPass* card or device being captured are low and are considering not using the "capture card" authorization response for transactions from *PayPass* cards and devices.

3.4 Delivering a Quality MasterCard *PayPass* Experience

The requirements and recommendations identified in Sections 3.1 to 3.3 are key to delivering what MasterCard calls "a quality MasterCard *PayPass* experience," namely, one where *all* elements of the payment process have been optimized for simplicity and speed. By making all MasterCard *PayPass* transactions a quality experience for all merchants and card or device users, the conversion of transactions from cash to card will be accelerated.

4. PROCESSING MASTERCARD *PAYPASS* TRANSACTIONS

This section describes the payment processing requirements specific to MasterCard *PayPass*—Mag Stripe transactions.

A *PayPass* transaction is processed in the same way as a regular magnetic stripe transaction. The only difference is that it must be coded to indicate that it was tapped, as opposed to swiped or keyed, and to indicate if the POS was *PayPass*-enabled or not (regardless of how the transaction was initiated).

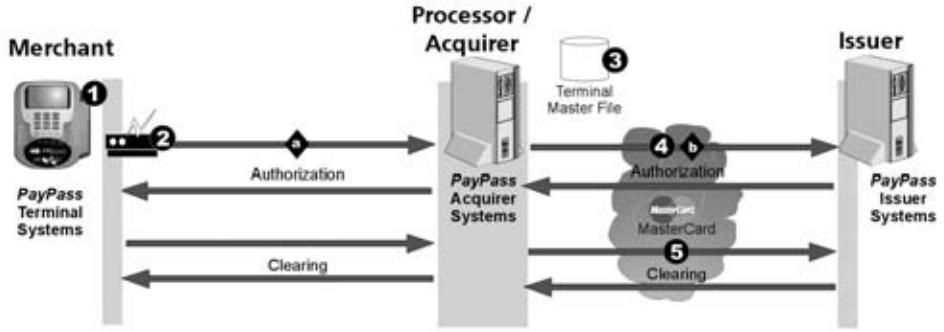


Figure 18, MasterCard *PayPass* Payment Processing

1. MasterCard *PayPass*–capable terminal reads *PayPass* card or device data and sends it for authorization. Data includes indication that transaction was tapped, swiped, or keyed.
2. High-speed authorization system transmits authorization request to the acquirer.
3. If not provided in the authorization message to the acquirer, the acquirer determines if the POS is *PayPass* enabled, for example using a terminal master file.
4. Acquirer codes the POS entry mode and terminal capability elements of the appropriate MasterCard authorization message as specified by MasterCard, using information from the terminal systems and the terminal master file. For *PayPass* transactions, the data will reflect that it was supplied by a terminal that is *PayPass* enabled and that the data was communicated via the terminal's contactless interface.

   The transaction is then transmitted to the card issuer via MasterCard's authorization network.
5. A similar process to 3 and 4 above occurs for the clearing request to MasterCard's systems. This data includes an indication of the transaction's POS entry mode (DE 22) and terminal capability (DE 61).

   The following MasterCard Global Operations Bulletin describes the coding requirements: No 6, 1 June 2005.

5. IMPLEMENTING MASTERCARD *PAYPASS*

This section offers advice and guidance on implementing MasterCard *PayPass*. It explains what changes are needed to acquirers' card payment processing/acquiring systems and processes in order to accept *PayPass*.

MasterCard *PayPass* is designed to make use of existing authorization and clearing message formats in order to minimize the changes needed to be made by an acquirer.

In order to support *PayPass* transaction processing, as described in Section 4, acquirers must typically complete the following:

- Register merchant, if eligible, in the MasterCard QPS program if they are not already registered. (The QPS program exists in a limited number of markets, including the U.S. and Canada, and is open to select merchant categories.)

NOTE

Not all merchant categories are eligible to join the QPS program but they can still support *PayPass*.

- Upgrade the merchant authorization connection to high-speed lines, if one is not already installed.
- Update records to reflect the extended terminal capability to indicate that the terminal can accept *PayPass* transactions. This record will be a reference point for acquirers to submit accurate values in the authorization and clearing messages.
- Support the requirement to populate the POS entry mode identifier by supplying entry mode information from POS terminal/ECR to processing systems. How this is achieved is up to the acquirer.
- Code the POS entry mode and POS Card Data Terminal Input Capability in the authorization and clearing records that are transmitted to MasterCard.
- Fully test the implementation to ensure that *PayPass* transactions are processed correctly.
- Update transaction reporting capabilities, including reports provided to merchants, to specifically identify *PayPass* transactions.
- Educate merchants on identifying *PayPass* cards and devices, especially on the fact that some devices may not have a traditional signature panel.
- Complete all necessary testing to gain MasterCard approval for each merchant implementation as defined in the current *MasterCard PayPass Approval Processes for Acquirer and Merchant Implementations*.

Appendix A, Global Operations Bulletin No. 6, 1 June 2005

Data Element Values for MasterCard PayPass

Simon Phillips, Vice President, Product Management

Suggested routing: Authorization Contact, Chip Technology Contact, Clearing Contact, Compliance Contact, Data Center Contact, Principal Contact, Programming Contact, Security Contact, Settlement Contact

Applies to: ☑ Issuers ☑ Acquirers ☑ Processors

Summary: MasterCard is clarifying the mandatory requirements for use of correct data element values in authorization and clearing messages for credit, and financial request messages and reconciliation files for debit for MasterCard *PayPass*™ (proximity/chip-read) transactions.

Action Indicator:
T Testing required
R Member must register to have access to product or service

Effective Date: Immediately

MasterCard is clarifying the mandatory requirements for use of correct data element values in authorization and clearing messages for credit, and financial request messages and reconciliation files for debit for MasterCard *PayPass*™ (proximity/chip-read) transactions.

Background

As announced in *Global Operations Bulletin* No. 8, 1 August 2003 MasterCard launched MasterCard *PayPass*, a new contactless/proximity payment program that provides consumers with a simpler way to pay. Using MasterCard *PayPass*, consumers simply tap their payment card or device against a specially equipped merchant terminal. Payment details are transmitted wirelessly from the card to the terminal, eliminating the need to swipe the card through a reader. *PayPass* is ideal for traditional cash-only environments where speed is important, such as fast food restaurants and movie theaters.

Previous details of these requirements were published in:

- *Global Deposit Access Bulletin* No. 6, 21 June 2004
- *Global Operations Bulletin* No. 9, 2 September 2003

- *Global Operations Bulletin* No. 2, 1 February 2005
- *GCMS Release 05.2 Document*

This article clarifies previously published information concerning the requirements for providing specified values in the authorization and clearing messages and debit messages for *PayPass*/proximity chip-read transactions.

Credit authorization

MasterCard requires that *PayPass* transactions must be coded as follows for credit authorization:

Data Element 22

Data Element (DE) 22 (Point of Service [POS] Entry Mode), subfield 1 (POS Terminal Primary Account Number [PAN] Entry Mode), must contain:

- The value of "91" indicating PAN auto-entry mode via contactless magnetic stripe (*PayPass*-Mag Stripe)
- The value of "7" indicating PAN auto-entry via contactless M/Chip (*PayPass*-M/Chip)

Data Element 61

DE 61 POS Data, subfield 11 (POS Card Data Terminal Input Capability), must contain:

- The value of "4" to indicate contactless magnetic stripe (*PayPass*-Mag Stripe only capability, for example, No *PayPass*-M/chip capability)
- The value of "3" to indicate contactless M/Chip (*PayPass*-M/Chip and *PayPass*-Mag Stripe capability - Both can be processed)

Note that a *PayPass* M/Chip card/device can be accepted at a *PayPass* Mag Stripe terminal. In this instance the M/Chip card/device emulates a *PayPass* Mag Stripe card/device.

These details are also available in the *Customer Interface Specification* manual.

Member requirements for credit authorization

MasterCard requires that:

- Acquirers, processors, and the merchants they support update their systems to send these values

Appendix A, Global Operations Bulletin No. 6, 1 June 2005—continued

- Issuers must be prepared to receive the DE 22 values if they issue *PayPass* cards or devices
- Issuers must be prepared to receive DE 61 values even if they ***do not*** issue *PayPass* cards or devices.

Credit clearing

MasterCard requires that *PayPass* transactions must be coded as follows for credit clearing:

DE 22, subfield 1

DE 22, subfield 1 (Terminal Data: Card Data Input Capability) must contain:

- The value of "A" indicating Clearing Proximity Chip Online transaction (*PayPass*-Mag Stripe only capability, [No *PayPass*-M/Chip capability])
- The value of "M" to indicate Clearing Proximity Chip EMV transaction (*PayPass*-M/Chip and *PayPass*-Mag Stripe capability [Both can be processed])

Note that a *PayPass* M/Chip card/device can be accepted at a *PayPass* Mag Stripe terminal. In this instance the M/Chip card/device emulates a *PayPass* Mag Stripe card/device.

DE 22, subfield 7

DE 22, subfield 7 (Card Data: Input Mode) must contain:

- The value of "A" indicating PAN auto-entry mode was via contactless magnetic stripe (*PayPass*-Mag Stripe)
- The value of "M" indicating PAN auto-entry mode was via contactless M/Chip (*PayPass*-M/Chip-contactless M/Chip)

As announced in *Global Operations Bulletin* No. 2, 1 February 2005, effective with *GCMS Release 05.2 Document*, MasterCard revised the Standards for DE 22 within all First Presentment 1240/ clearing messages. The values for DE 22 in the authorization message must be mapped to the First Presentment/1240 record, as defined in the release document and in the *IPM Clearing Formats* manual in chapters 4 and 5.

Member requirements for credit clearing

MasterCard requires that:

- Acquirers, processors, and the merchants they support update their systems to send these values.

- Issuers must be prepared to receive the values in DE 22, subfield 7, if they issue *PayPass* cards or devices
- Issuers must be prepared to receive the values in DE 22, subfield 1, even if they ***do not*** issue *PayPass* cards or devices.

Debit

Card issuers may add *PayPass* to MasterCard debit cards. To support the requirements necessary to identify these transactions, the MasterCard® Debit Switch (MDS) now supports specific values in the financial request message and in the new 250-byte reconciliation file.

Debit requirements

MasterCard has included two values in DE 22, that indicate the method used to enter the PAN into the terminal, and two values in DE 61 that indicate the terminal input capability. These requirements apply both to members that are serviced through the MDS and all other debit networks and processors.

Other debit networks and processors

For other debit networks and processors, the above values may be mapped to other data elements within their proprietary message formats. MasterCard recommends that members contact their debit network, processor, or both, to determine the changes to those interfaces.

MasterCard also recommends that issuers contact their debit network or processor when offering *PayPass* functionality to cardholders, to ensure availability of these indicators across all networks.

Debit PayPass transactions

MasterCard requires that *PayPass* debit transactions must be coded as follows:

DE 22

Point-of-Service (POS) Entry Mode - DE 22, subfield POS Terminal PAN Entry Mode, positions 1-2, must contain:

- The value of "91" indicating PAN auto-entry mode via contactless magnetic stripe (*PayPass* - Mag Stripe). The edits for value "91" are the same as the edits for when DE 22, subfield 1 = "90"

Appendix A, Global Operations Bulletin No. 6, 1 June 2005—continued

- The value of "07" indicating PAN auto-entry via contactless M/Chip (*PayPass* - M/Chip). The edits for value `07' are the same as the edits for when DE 22, subfield 1 = "05"

DE 61

Point of Service (POS) Data - DE 61, subfield POS Card Data Terminal Input Capability Indicator, position 11, must contain:

- The value of "4" to indicate contactless magnetic stripe (*PayPass* - Mag Stripe only capability. i.e. No *PayPass* - M/Chip capability).
- The value of "3" to indicate Contactless M/Chip (*PayPass* - M/Chip and *PayPass* - Mag Stripe capability. i.e. Both can be accepted).

Note that a *PayPass* M/Chip card/device can be accepted at a *PayPass* Mag Stripe terminal. In this instance the M/Chip card/device emulates a *PayPass* Mag Stripe card/device.

Member requirements for debit

MasterCard requires that:

- Acquirers, processors, and the merchants they support update their systems to send these values
- Issuers must be prepared to receive the values in DE 22 if they issue *PayPass* cards or devices
- Issuers must be prepared to receive the values in DE 61 even if they ***do not*** issue *PayPass* cards or devices.

Testing

Acquirers and merchants must test compliance with these requirements for their systems, and for each new terminal type or terminal type version using MasterCard test cards (ETEC6). For credit, acquirers and merchants should use the online Member Test Facility (MTF—Credit) and the MasterCard Credit Authorization Simulator, debit, acquirers and merchants should use the online Debit Test Facility (DTF—Debit) and the MasterCard Debit Authorization Simulator.

Please contact your normal operation support to schedule testing and to obtain a test card package.

For more information

For more information about this article, please contact your Customer Implementation Services representative.

For more information on MasterCard *PayPass*, please contact:

E-mail: paypass@mastercard.com

Appendix B, Glossary

Term	Description
2D Device	This term is used to describe the physical characteristics of the device such that, as per traditional ISO 7810 cards, the length and breadth of the device are significantly greater than its thickness. The thickness is uniform across the device and is similar to ISO 7810 cards (e.g., a *PayPass* 2D fob device).
2D Fob	A 2D *PayPass* device that is manufactured in the form of a traditional card (ISO 7810) but ends up as a different size and shape. Typically, a *PayPass* 2D fob will be either die-cut from a full-size card after personalization or a score is made in the card plastic such that it can be snapped out by the consumer after fulfillment.
3D Device	This term is used to describe the physical characteristics of the device such that, unlike traditional cards, the thickness of the device is noticeable and of similar magnitude to its other dimensions (e.g., a *PayPass* 3D fob device).
3D Fob	A 3D *PayPass* device.
3DES	Triple DES Cryptographic Algorithm. An enhanced cryptographic algorithm, based on the DES Cryptographic Algorithm, adopted by the National Bureau of Standards for Data Security.
Account Number	The 16-digit identifier of a credit or debit card.
Acquirer	Member of MasterCard International involved in signing and servicing merchants that accept MasterCard.
Antenna	Coil of wire through which RF energy is provided.
Application File Locator (AFL)	Identifies the records available to the application and the reference to their location in files in the chip card's memory.
Application Identifier (AID)	Identifier of an application in the chip card, coded in hexadecimal.

Term	Description
Application Interchange Profile (AIP)	Indicator of the capabilities of the chip card to support specific functions.
Application Transaction Counter (ATC)	A mechanism for tracking the transactions done using a specific account; used to prevent fraudulent use or cloning of a card or device.
Authorization	The process of confirming that a payment account is valid and is approved.
Broadband	A network connection with capacity to send and receive large amounts of data relatively quickly (vs. dial-up).
Card	Plastic form factor compliant with ISO 7810 that contains a payment application coded on a magnetic stripe.
Card Authentication Method (CAM)	Method used to verify that a card or device is genuinely the one issued to the consumer.
Card or Device Holder	See Consumer.
Card Verification Code 1 (CVC1)	A code contained in a card's magnetic stripe data that verifies a specific card is physically present at the POS; used to reduce the risk of counterfeiting fraud.
Card Verification Code 2 (CVC2)	Value generated by the issuer and printed on a signature panel on the back of the card; implemented for manual (visual) use during MOTO and e-commerce transactions.
Card Verification Code 3 (CVC3)	Value used in place of CVC1 in the Discretionary Data field of the Track 1 and 2 data for MasterCard *PayPass* transactions; usually a dynamic cryptogram generated by the card or device, but may be a static cryptogram.
Certification	The process of confirming that a card, device, reader, terminal, or software application is approved for use.
Chargeback	A transaction disputed by the consumer or issuer that is represented back to the merchant.
Clearing	The process of remitting a sales draft for settlement.

Appendix B, Glossary—continued

Term	Description
Companion Card	An ISO-compliant MasterCard card with which a companion *PayPass* device shares a single MasterCard account relationship between the issuer and the consumer.
Compute Cryptographic Checksum (CCC)	Card/device command supported for *PayPass*—Mag Stripe transactions; returns the CVC3 value for the transaction.
Consumer	The payment accountholder to whom the *PayPass* card or device is issued.
Consumer Verification Method (CVM)	Method used to verify the identity of the payment accountholder.
Contactless Chip	The RF chip found inside a *PayPass* card or device; when connected to an antenna, it permits card or device transactions without swiping the magnetic stripe.
Data Element 22	The portion of a MasterCard authorization message that denotes how the account number was read/entered into the POS device (e.g., magnetic stripe read, key entered, read via a *PayPass* reader).
Data Element 61	The portion of a MasterCard authorization message that denotes the various capabilities of a POS terminal (e.g., equipped with mag stripe reader, smart card reader, etc.).
Electronic Cash Register (ECR)	Cash register that is integrated with payment acceptance tools and/or order system.
Embedded Device	A *PayPass* device that is manufactured to be contained in a consumer device such as a watch or a cell phone.
File Control Information (FCI)	The string of data bytes available in response to a SELECT command.
Floor Limit	The preset amount under which a transaction does not require online authorization.
Form Factor	The physical characteristics of a device, including its size and shape.

Term	Description
Help Desk	A call center dedicated to assisting users with a technology (e.g., a merchant help desk might provide information to merchants when they experience difficulty with a terminal).
Implementation Plan	A plan that maps the implementation of a project and all the steps required to achieve this.
Integrated Circuit Card (ICC)	The ISO/IEC term for a chip card/device or a smart card.
International Standards Organization (ISO)	An international organization that sets standards for technology to assure that products are interoperable from one country to the next.
Issuer	Member of MasterCard International that issues MasterCard payment accounts to their consumers.
Kiosks	Locations where consumers interact with or without the oversight of a clerk or merchant staff person.
Linked Card	See Companion Card.
Magnetic Stripe (Mag Stripe)	Reference to a conventional (ISO/IEC 7810) magnetic stripe as defined and used by the MasterCard network.
Magnetic Stripe Reader (MSR)	The part that physically reads the data encoded on a card's magnetic stripe.
Member	Financial institution registered as a member of MasterCard and involved in issuing or acquiring activity.
Merchant	An organization accepting cards or devices as a payment instrument. Has a relationship with an acquirer.
***PayPass* Application**	The software that executes on a *PayPass* chip.
***PayPass* Card**	A proximity device containing a *PayPass* chip and application that has the characteristics of the traditional bankcard form factor, as specified in ISO 7810.

Appendix B, Glossary—continued

Term	Description
***PayPass* Card (or Device)**	Card (or device) provided by an issuer containing a contactless chip that uses RF, supplied via an antenna, to run a *PayPass* application configured for a consumer.
***PayPass* Chip**	The integrated circuit chip contained within a *PayPass* card or device that executes the *PayPass* application.
***PayPass* Coupling Device (PCD)**	The *PayPass* reader utilizes an inductive coupling, energizing RF field to both power the *PayPass* card or device and control data exchange when modulated. PCDs typically have an operating range of less than 4 inches and may form part of a merchant terminal.
***PayPass* Payment System Environment (PPSE)**	The list of contactless applications, indicated through their AID, available on a *PayPass* card.
Personal Identification Number (PIN)	A number used by an issuer to authenticate a consumer (a type of CVM).
PIN Pad	A numeric keypad into which a consumer can type a PIN.
Point of Sale (POS)	The point where a consumer pays for merchandise; may encompass a cash register, card or device terminal, *PayPass* reader, etc.
Primary Account Number (PAN)	See Account Number.
Processing Options Data Object List (PDOL)	List of data objects that the terminal should provide to the card or device.
Proximity Coupling Device (PCD)	The *PayPass* reader or terminal.
Proximity Device	A consumer device that can be read from a distance (within a specified range) without physical contact. *PayPass* cards and devices are proximity devices.
Quick Payment Service (QPS)	A MasterCard program that allows approved merchants in certain merchant category codes to accept transactions under US $25 without a consumer signature.

Term	Description
Quick-Service Restaurant (QSR)	A restaurant where consumers are served food quickly, either via drive-thru or at a counter.
Radio Frequency (RF)	A technology that allows two devices to communicate via radio waves.
Read	The act of a MasterCard terminal communicating with a MasterCard card or device and receiving consumer payment data; this may be via the magnetic stripe swipe process or from a *PayPass* RF interaction.
Reader	Refers to the terminal component that communicates with the *PayPass* card or device to receive the required information and transmit it to the POS payment application.
Serial/RS232 Port	A physical hardware interface on a PC, ECR, terminal, or other electronic device used to connect peripheral devices.
Settlement	The process by which an issuer pays an acquirer for transactions made by its consumers.
Stand-alone Terminal	Terminal that is not integrated with a cash register.
Static CVC3	A CVC3 value calculated using a CVC1 algorithm, but using different input data to generate a value that differs from CVC1.
Terminal	Term often used to refer to a POS device.
Transaction	A payment for goods or services.
Unpredictable Number (UN)	A number generated by the *PayPass* reader that cannot be calculated or predicted in advance.
USB Connections	A physical hardware interface on a PC, ECR, terminal, or other electronic device used to connect peripheral devices.
Vendor	A company that sells terminals or other goods or services.

www.paypass.com

For questions e-mail
paypass@mastercard.com

MasterCard International