U.S. Merchant Acceptance Guide

17 December 2010

Notices

Proprietary Rights

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

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

Trademarks

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

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

Billing

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

Information Available Online

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

Translation

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

Publication Code

MAG

Table of Contents

Chapter 1 Introduction

This chapter contains information to help you use this document.

Overview

The *U.S. Merchant Acceptance Guide* provides guidelines and best practices for merchants in the U.S. region that accept MasterCard cards.

MasterCard provides this guide to merchants and their staffs.

MasterCard Merchant Web Site

MasterCard hosts an interactive and engaging Web site for merchants. For more information about merchant acceptance solutions, resources, and payment solutions, visit www.mastercard.com/us/merchant.

MasterCard Standards

The MasterCard Worldwide Network operates under specific Standards that may be amended from time to time. These Standards inform, guide, and provide clarity to all of its members, processors, and merchants.

As a MasterCard merchant, you have access to the MasterCard Standards posted on the MasterCard Merchant Web site and should understand applicable MasterCard Standards and how they apply to your business. These documents are available at www.mastercard.com/us/merchant.

NOTE

MasterCard Standards change frequently. While MasterCard strives to keep these documents up to date, it is possible that they will not always be absolutely current in all regards. In the event of any discrepancy between the documents provided to merchants online and Standards MasterCard deems to be the current and in effect, the Standards as deemed in effect by MasterCard will apply.

Contents

The following information provides an overview of this guide:

- **Getting Started**—Explains the benefits of accepting MasterCard cards and provides information on how to accept MasterCard cards and choose an acquirer. Answers to common business questions for new or prospective merchants are included as well.
- **Merchant Acceptance**—Explains types of MasterCard cards, products, services, and programs that can help you prosper. Information about merchant rules and responsibilities and additional information that may help answer general merchant questions about card acceptance are also provided.
- **Transaction Processing**—Provides an overview of how MasterCard transactions are submitted. Information about MasterCard systems and the participants in a typical transaction is also included.
- **Card Security**—Provides card security requirements and recommendations, information about security and card verification programs, and MasterCard card identification features.

- **Interchange**—Explains interchange and interchange rates established by MasterCard.

- **Chargeback Support**—Provides a high-level overview about chargeback requirements and best practices.

- **Controlling Fraud**—Explains types of card fraud and provides information to help merchants prevent fraud. Also provides a merchant fraud checklist.

- **Glossary**—Provides a glossary of terms, concepts, acronyms, and abbreviations used in the *Merchant Acceptance Guide*.

Related Information

The following documents and resources provide information related to the subjects discussed in this guide:

- *Chargeback Guide*
- *Interchange and the Payments Industry Fact Sheet*
- *Interchange Myths and Facts*
- *Maestro Global Rules*
- *MasterCard PayPass Brochure*
- *MasterCard Rules*
- *MasterCard SecureCode Brochure*
- *MasterCard Worldwide U.S. and Interregional Interchange Rates*
- *POS Terminal Security Program—Approval List*
- *POS Terminal Security Program—Program Manual*
- *Quick Payment Service Program Guide*
- *Security Rules and Procedures—Merchant Edition*

Chapter 2 Getting Started

This chapter explains the benefits of accepting MasterCard cards and provides information on how to accept MasterCard cards and choose an acquirer. Answers to common business questions for new or prospective merchants are included as well.

Value of Accepting MasterCard Cards

MasterCard is constantly developing sophisticated payment technologies that are focused on improving the way you do business with your customers.

Whether you're a new business or an established enterprise, accepting MasterCard will likely have a big impact on your bottom line. Some of the most significant benefits include:

- **Increased sales**—Consumers spend more when they're not constrained by cash on hand. You may see increased purchases of higher-margin products, as well as specialty items. And customers may visit your store more often.
- **Customer satisfaction**—Your customers will appreciate the fact that you allow them the flexibility to pay the way they want to pay—including by credit or debit card.
- **Speed of checkout**—You'll speed your customers through checkout with rapid electronic payment. No more counting change or waiting while customers write checks.
- **Improved efficiency**—Card transactions today are conducted electronically. These paperless payments can save you time and money by minimizing cash handling and payment reconciliation, giving you more time to manage and grow your business.
- **Safety**—With lower volumes of cash, you're less vulnerable to theft and pilfering.
- **Currency conversion**—Electronic payments on MasterCard® and Maestro® cards are settled in the currency in which you sell your goods and services, regardless of where the cardholder is from. If you sell in U.S. or Canadian dollars, that's how you'll be paid.
- **Customer recognition of the MasterCard brand mark**—The bold MasterCard brand mark, with its bright look and visual impact, helps merchants worldwide take advantage of the profitable benefits of exterior signage.
- **Increased traffic, increased sales**—While interior signage is valuable, many customers rely on exterior signage to determine if a merchant accepts MasterCard cards. A window or door logo is an important tool that can lead to increased traffic and higher sales.
- **MasterCard logo may lead to increased profits**—When customers pay by MasterCard instead of paying by check, you may experience increased profitability that comes from reducing processing fees associated with paying by check and improved cash flow with MasterCard payments versus checks because card transactions are typically settled in 24 to 72 hours.
- **MasterCard signage means a big opportunity**—MasterCard signage is a competitive advantage. Letting cardholders know you accept MasterCard can lead to increased traffic and sales volume.

How to Accept MasterCard Cards

It's easy to begin to accept MasterCard cards. MasterCard offers easier, more convenient credit, debit, and prepaid payment options for your customers. Follow these quick and simple steps to become a MasterCard merchant.

Step 1: Register for the Referral Program

To obtain a customized list of acquirers/MSPs registered with MasterCard, you must enroll in the Referral Program.

An acquirer or member service provider (MSP) acts as your liaison to MasterCard. An acquirer is a licensed MasterCard member (that maintains the merchant relationship and acquires the data relating to a transaction from the merchant or card acceptor) that provides services, such as card payment processing, hardware and software, monthly statements, and more. An MSP is a third party contracted by an acquirer to handle merchant services on the acquirer's behalf and may function as a sales agent for an acquirer. MSPs must be registered with MasterCard.

When you register in the Referral Program, you may be contacted by participating acquirers or MSPs via e-mail or telephone. If you do not want to be contacted, you may choose that option during the registration process.

Step 2: Log On and Review Acquirers/MSPs

Once you complete and submit your profile, log on to the Referral Program Web site using your user name and password to review the acquirer and MSP profiles that match your request.

Step 3: Set Up a Merchant Account

To apply for a merchant account, contact an acquirer or MSP of your choice.

MasterCard understands that there are many considerations to make when assessing the benefits of accepting MasterCard cards. For answers to common business questions about card acceptance, see Frequently Asked Questions.

How to Choose an Acquirer

The MasterCard Referral Program makes it easy for merchants to select a licensed acquirer. The Referral Program identifies acquirers and MSPs for merchants that are interested in accepting MasterCard cards as a payment option. This program is also designed to generate leads that will help you provide the high levels of service that merchants are demanding, as well as help you build your business.

Choosing an acquirer is an important step in accepting MasterCard. Your acquirer is the financial institution that will accept and process MasterCard transactions. Your acquirer can be a strong business ally as well.

The key parties involved in MasterCard transactions are:

- **Acquirer**—A licensed MasterCard member that maintains the merchant relationship and acquires the data relating to a transaction from the merchant or card acceptor.

* **Issuer**—A licensed MasterCard member that issues cards or access devices to accountholders.

NOTE

MasterCard is not an issuer.

When choosing an acquirer, consider these important factors:

* **Payment card industry guidance**—Select an acquirer that is ready and eager to provide you guidance through the issues, challenges, and technical details of the payment card industry.

* **Industry/vertical market experience**—Select an acquirer that has experience in your industry or vertical market. These acquirers understand the needs and conditions of your business.

* **Tools and technology**—Engage the acquirer about the tools, technology, and services it supports that are particularly relevant to your business. For example, it may be important to know if the acquirer supports technology that makes transactions faster and more convenient at the point of sale. Additionally, consider what factors affect your cost of acceptance (electronic vs. manual entry; vertical-specific incentive programs).

* **Security**—Ask the acquirer what its policies and practices are regarding fraud avoidance. The acquirer should have a clear and multi-faceted approach that involves technology—such as MasterCard *SecureCode*™ acceptance—and best practices.

* **Chargeback management**—Ask the acquirer what its policies and procedures are for chargeback management. Chargebacks usually happen when there is a customer dispute or an error and/or the dollar value of the transaction—and financial liability—is typically reversed back to the merchant.

To view or print a list of participating acquirers and MSPs, go to www.mastercard.com/us/merchant and submit your completed profile.

Frequently Asked Questions

The following information may help answer common business questions about card acceptance for a new or prospective merchant.

What is a merchant?—A merchant is a commercial entity or person that pursuant to a merchant agreement is authorized to accept cards and access devices when properly presented.

What is the credit/debit business and how does it work?—Merchants can accept a MasterCard credit card or a MasterCard debit card. A credit product allows the consumer to make purchases based on a line of credit established by their issuer. The credit limit is the spending amount established by the issuer based on a consumer credit profile. A debit product allows the consumer to make a purchase based on funds available in their bank account. Debit purchases are drawn directly from the consumer's bank account and show up directly on the consumer's monthly bank statement.

How do I begin accepting MasterCard cards?—Contact an acquirer or member service provider (MSP) to apply for a merchant account. An MSP is a third party contracted by some acquirers to handle merchant services on the acquirer's behalf and may function as a sales agent for an acquirer. MSPs must be registered with MasterCard.

Who is an acquirer and why do I need one?—An acquirer is a licensed MasterCard member that maintains the merchant relationship and acquires the data relating to a transaction from the merchant or card acceptor. The acquirer is set up to connect and process transactions over the MasterCard Worldwide Network. Acquirers or MSPs either sell their processing services directly to merchants or hire agents to sell on their behalf. However, these agents must be registered with MasterCard and clearly identify the MasterCard member they represent on their business cards and stationery. The merchant agreement must also have the name of the bank clearly identified.

How long does it take before I can start accepting MasterCard cards?—This depends on your acquirer and the type of business you manage. Usually, you can get set up to accept MasterCard cards in less than a month.

Will I incur any costs?—Yes. The costs you will incur will be quoted to you by the acquirer.

What is an interchange rate?—MasterCard interchange rates are established by MasterCard, and are fees paid by acquirers to issuers on purchase transactions conducted on MasterCard cards. Interchange fees are only one of many cost components included in a Merchant Discount Rate and are a necessary and efficient method by which MasterCard maintains a vibrant payments network.

What are the benefits of accepting MasterCard?—Whether you're a new business or an established enterprise, card acceptance will likely have a big impact on your bottom line. For more information about benefits, see Value of Accepting MasterCard Cards.

Are there any programs that will help to grow my business?—Depending on the type of merchant business you run, MasterCard has many programs designed to grow your business. For more information about this collection of programs, visit www.mastercard.com/us/merchant.

Who do I call if I have a problem with my terminals? Contact the acquirer or MSP that set you up to accept MasterCard cards.

What type of card programs does MasterCard offer?—MasterCard provides innovative payment solutions to consumers and companies around the world. For more information about MasterCard innovative payment solutions, see Types of Cards.

Chapter 3 Merchant Acceptance

This chapter explains types of MasterCard cards, products, services, and programs that can help you prosper. Information about merchant rules and responsibilities and information that may help answer general merchant questions about card acceptance are also provided.

MasterCard Product Solutions

MasterCard payment solutions offer convenience and flexibility for you and your customers. They can also help to increase the potential number of transactions that you can process—more transactions equal higher revenues.

Business is never really "business as usual." It's a competition. It means taking advantage of opportunities as they come, recognizing customer behavior before it becomes a trend, and keeping pace with your competition.

MasterCard has developed innovative payment products and services that can give your customers faster, more enjoyable experiences while providing real benefits for your business:

- MasterCard Electronic™ reduces risk by promoting electronic processing of transactions.
- MasterCard® *PayPass*™ speeds checkout, improves customer service, and can potentially increase the number of customers you can serve.
- The enhanced security of MasterCard *SecureCode*™ can increase online sales and reduce fraud and chargeback costs. For information about *SecureCode*, see MasterCard SecureCode.
- Co-branded cards offer a potent marketing opportunity and enhanced customer loyalty.

Some, or all, of these solutions can help to give you the competitive advantages you need to win.

MasterCard Advisors Merchant Solutions

MasterCard Advisors Merchant Solutions is designed to help merchants to stay ahead of their competition and maximize their opportunities—providing valuable business intelligence and applications that can help improve market share and capture more spending from your customers.

The tools in the suite—SpendingPulse™, Benchmark Analytics, and Custom Marketing Solutions—provide you with the knowledge and tools you need to improve performance. You can benefit from unique and timely information on consumer spending, or performance data on your stores benchmarked against your larger industry and a defined competitive set. Further, our marketing solutions identify patterns of consumer behavior, indicating a likelihood to respond to your promotional offers, and then reach out to those customers and prospects with direct marketing featuring your brand identity.

These tools, whether deployed individually or in combination, help enhance your ability to:

- Maximize promotional, geographic, and merchandising opportunities
- Understand consumer demand and market share so you can manage inventory and staff appropriately and maximize operational efficiency
- Attract new customers, enhance consumer loyalty, and capture more consumer spending

SpendingPulse

SpendingPulse™ reports give you a clear and detailed picture of consumer spending in your industry and at a macro level. Data is based on sales activity from the MasterCard payments network coupled with survey-based estimates for other payment forms, including cash and check. The result: exceptionally timely, actionable reports that can help you conduct more effective marketing campaigns, optimize forecasting and planning, and improve supply chain management.

Benchmark Analytics

Benchmark Analytics is a Web-based application that delivers comparative performance data directly to your desktop. Examine spending and growth in your locations—from the national to the MSA or DMA level—against overall performance in your industry category and against a defined, aggregated set of competitors. Track performance over time and across multiple loyalty-based segments for greater depth. The unique intelligence you gain can help you make important and productive decisions about advertising and marketing, buying, merchandising, and operations.

Custom Marketing Solutions

Custom Marketing Solutions are turnkey marketing programs aimed at your goals: customer acquisition, improved loyalty, or increased spending from existing customers. Using custom models and drawing on the cardholder lists of participating card issuers, we identify the best potential customers for your promotional offers, then develop and execute direct marketing programs on your behalf that encourage the specified behavior.

For more information about, visit www.mastercardadvisors.com or send an e-mail to advisorInfo@mastercardadvisors.com,

MasterCard Automatic Billing Updater

The MasterCard Automatic Billing Updater is a service that helps ensure uninterrupted payment for you and uninterrupted service for customers by seamlessly updating card-on-file account information. It maintains and builds customer satisfaction, making it less likely for customers to switch to another merchant.

If you maintain card-on-file data for your customers' automatic recurring bill payments, you face the challenge of card payments that decline due to account changes that have not been communicated to you with each billing period. Declines compromise revenue flow and are inconvenient to customers as well. They also increase your direct and indirect expenses by forcing you to contact customers for either updated account information or alternate payment arrangements.

By automatically maintaining the accuracy of customer card data, the MasterCard Automatic Billing Updater prevents disruptions due to account changes. It extends the life of online and offline automatic recurring payment arrangements by helping to secure these ongoing, revenue-generating relationships, while helping to lock in revenue, reduce processing costs, maintain service continuity, and strengthen cardholder satisfaction.

Benefits

Merchants who use the MasterCard Automatic Billing Updater service see the following benefits:
- Decreased operating and processing cost
- Increased customer satisfaction
- Improved funds collection
- Prevention of exception processing

How It Works

1. Participating issuers submit their account changes to the Automatic Billing Updater database.
2. Registered merchants submit their billing files inquiries to their acquirer.
3. Acquirers submit the billing file inquiries to the Automatic Billing Updater database.
4. MasterCard processes the merchant account inquiries against issuer account change submissions, and then returns results to the acquirers.
5. Acquirers return updated account inquiries records to their specific merchants.
6. Merchants update their billing files with the changed account information, and have more successful billing.

The following illustration shows how the Automatic Billing Updater works.
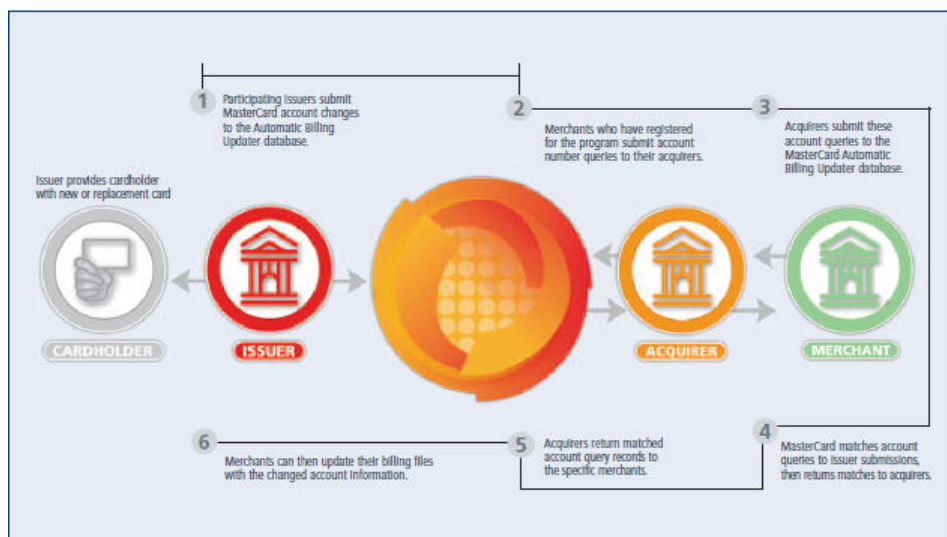
For more information, contact your MasterCard representative.

Types of Cards

Giving your customers a variety of easy, time-saving payment options is good for your business. You want to create the most positive experience possible for your customers, giving them a significant reason to choose your business over your competitors. MasterCard has created several branded product solutions that can help you do just that.

MasterCard Cards

MasterCard® consumer cards provide flexible payment options, convenience, and security for consumers around the world. Our Standard, Gold, Platinum, and World, and Unembossed MasterCard® credit cards are accepted at over 30 million locations worldwide (total MasterCard acceptance locations as of September 2010). Consumers look for the MasterCard brand wherever and whenever they shop for products and services.

Unembossed MasterCard Cards

Unembossed cards are like other MasterCard cards with one difference—the letters and numbers on the cards are "flat." All account information is printed rather than embossed with raised letters and numbers. All other required card design features remain the same. In addition to promoting electronic transactions, unembossed cards allow for innovative card designs with various formats for the account information and better accommodation of applications, such as MasterCard® *PayPass*™ radio frequency identification (RFID) components.

Unembossed MasterCard cards may be accepted by any merchant that already accepts MasterCard cards and is equipped with a terminal capable of reading a magnetic stripe or chip. If you do not have a terminal capable of reading a magnetic stripe or chip and the customer is present, you may ask for another MasterCard form of payment.

If you are a merchant that processes transactions using only manual imprinters, you may not be able to accept this type of card yet, as you may incur additional liability in a chargeback situation. When a cardholder presents a card in person and if you choose to key-enter the cardholder account number into your point-of-sale (POS) system for authorization, you could be liable for certain chargebacks because you are not able to prove card presence through a manual imprint of the card. Details are available in the *Chargeback Guide*.

How to Recognize an Unembossed MasterCard Card

The following illustration shows how to recognize an unembossed MasterCard®
card.

How to Accept an Unembossed MasterCard Card

The following illustration shows how to accept an unembossed MasterCard® card.

1. A customer presents the unembossed MasterCard card for payment. A chip* or MasterCard® *PayPass*™ capability may be included on the card in some cases.

2. The card surface is flat, with no raised letters or numbers, so just check for the MasterCard Brand Mark and account information such as cardholder name, account number, expiration date and security elements.

3. Process the transaction using your terminal with the usual steps to complete the sale.

4. Ask the customer to sign the sales receipt or enter a PIN if required.

5. Compare the signature (if required) on the sales receipt with the signature on the card or confirm the terminal accepted the PIN.

6. Give the customer the merchandise, sales slip, and unembossed MasterCard card. The transaction is complete!

* Chip acceptance procedures apply.

If you do not have an electronic terminal, it is not functioning, or the card is damaged so it cannot be read electronically, ask for another form of MasterCard payment to complete the transaction.

When a cardholder presents a card in person and if you choose to key-enter the cardholder account number into your point-of-sale (POS) system for authorization, you could be liable for certain chargebacks because you are not able to prove card presence through a manual imprint of the card.

MasterCard Electronic

MasterCard Electronic™ is a 100 percent issuer-authorized payment solution that provides remarkable flexibility, security, and control. It is designed to help build your business by offering access to a whole new customer base from emerging segments while reducing risk. While MasterCard Electronic cards look different (the account information is printed without raised numbers or letters), they are a valid form of payment for electronically verified transactions.

MasterCard Electronic cards offer merchants the following benefits:

- **Incremental revenue and growth**—MasterCard Electronic can help you increase revenue through previously untapped customer segments and local and international transactions.

- **Enhanced control features**—MasterCard Electronic cards have no raised numbers or letters, so offline transaction risk is eliminated.

- **Cash and check conversion**—MasterCard Electronic can help you realize a reduction in cost and risk of cash and check handling.

- **Easy implementation**—MasterCard Electronic uses the existing Authorization Platform with virtually no changes in the clearing and settlement process.

- **Unique features**—MasterCard Electronic features:
  - 100 percent issuer authorized
  - No floor limit
  - No manual key entry
  - No call referrals
  - E-commerce transactions require MasterCard® *SecureCode*™
  - No mail order or telephone order transactions

MasterCard Electronic can help you reach customers who have not had access to traditional payment cards, potentially increasing revenue. Featuring remarkable flexibility, security and control, it's a versatile payment solution designed to encourage electronic transactions and help financial institutions and merchants build their businesses while reducing risk.

MasterCard Electronic cards have been specifically designed for use in electronic terminals. Cardholder information is printed, not raised, so the card cannot be used in a manual imprinter. The "100% ELECTRONIC" legend under the brand mark reinforces that message so consumers understand that merchants will be processing their transactions electronically.

A MasterCard Electronic card works just like any other MasterCard card at a point-of-sale with an electronic terminal. If you have an electronic data capture terminal, you are already eligible to begin accepting these cards, without equipment or system changes. However, because additional licensing is required to accept MasterCard Electronic cards, you will need to contact your acquirer or MSP to make sure they have already signed a MasterCard Electronic License Agreement.

Because MasterCard Electronic cards feature a distinctive brand mark, you will want to display a decal indicating that your establishment welcomes this brand. Free decals, as well as Brand Reference and Merchant Training lay-by cards, are available from your acquirer or MSP.

NOTE

MasterCard Electronic is only available to issuers outside of North America; therefore, merchants in the U.S. region may see MasterCard Electronic cards used by international customers.

Accepting MasterCard Electronic Cards

The following illustration shows how to accept a MasterCard Electronic™ card and complete the transaction.

MasterCard *PayPass*

MasterCard® *PayPass*™ is the industry's leading contactless payment system—customers never have to swipe their *PayPass*-enabled payment devices. A simple tap of a card, key fob, or mobile phone is all it takes for your customers to pay at checkout.[1]

Because *PayPass* is up to 20 percent faster than the average store transaction, you can serve more customers.[2] It's faster than cash and faster than traditional payment cards. For merchants, this payment system can mean significantly more potential sales each day, and for your customers, a more pleasant and valued experience.

PayPass offers your business a valuable competitive advantage and benefits including:

- Faster than cash and traditional magnetic stripe cards
- Serve more customers in less time
- Customers may spend more per transaction when they are not limited to cash on hand
- Improved speed and satisfaction promote customer loyalty
- Increased convenience sets you apart from competition
- Fewer cash transactions means less cash handled by your personnel

Customer Benefits

Customers also like the benefits that "tapping" affords:

- Simpler, faster, and more convenient than cash transactions
- No signature needed for purchases of USD 50 or less[1]
- Accurate recordkeeping—Purchases appear on cardholder's monthly statement
- Greater sense of security—Card never leaves the customer's hand
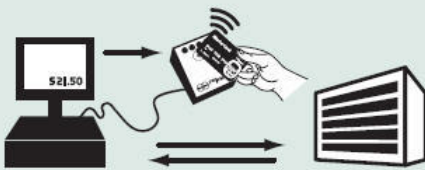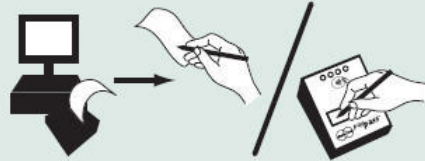
Processing a Typical *PayPass* Transaction

The following illustration shows the processing of a typical *PayPass* transaction.

---

1. Signature is not required for purchases of USD 50 or below at participating locations. PIN may be required for debit transactions.

2. Source: Issuer Case Studies conducted in 2009 and MasterCard *PayPass* Performance Insights. This data is derived from information provided to MasterCard and is subject to certain limited verification by MasterCard. Certain information indicated on the presentation may not have been independently verified by MasterCard. All data is subject to revision and amendment by MasterCard subsequent to the date of the release of this presentation.

CUSTOMER EXPERIENCE		TECHNOLOGY AT WORK
Cardholder sees amount due and recognizes that MasterCard *PayPass* is accepted for payment.		Transaction details are sent to the *PayPass*-enabled terminal from the electronic cash register (ECR).
Cardholder taps MasterCard *PayPass* card or device* on the terminal's *PayPass* reader. Visual and audible cues confirm card was read.		Terminal recognizes and activates *PayPass* card or device and exchanges payment account details. *PayPass* card or device generates unique transaction data all in less than half a second.
Cardholder waits a few seconds while transaction is authorized. With authorization, the terminal provides a second visual and audible cue.		Transaction data is transmitted to issuer along with payment account details via acquirer. Issuer receives data, checks unique transaction code, and authorizes transaction.
When required, customer signs a paper receipt or enters a PIN. For purchases of $50 or less, no signature is necessary; larger purchases will still require a cardholder signature. PIN may be required for debit.		After the transaction is complete, the point-of-sale system stores transaction information. Later, records are transmitted to acquirer for batch submission to the MasterCard network for clearing and settlement.

*This term refers to a cell phone, key chain tag, key fob, PDA, or other non-card payment device.

PayPass Equipment

There are several models of *PayPass* readers and terminals to choose from. When choosing your *PayPass* equipment, consider the following:

• Your physical location and business needs

• Available counter space

• Other environmental factors to consider such as outdoor locations

• Preference for a *PayPass*-only reader or a reader that also supports self-swiping?

For a complete list of available MasterCard tested, *PayPass*-approved products, go to www.paypass.com. For more information, contact your acquirer or member service provider (MSP), or send an e-mail to paypass@mastercard.com.

Accepting *PayPass*

Getting set up to accept *PayPass* is fast and efficient. To get started, visit www.mastercard.com/us/merchant or contact your acquirer or processor.

Maestro

The Maestro® PIN point-of-sale debit system lets consumers use their cards to make purchases as an alternative to cash or checks. By accepting PIN debit cards through Maestro ® International, the leading global debit solution, you can accept participating cards from around the country and around the world to maximize incremental sales and reduced handling costs.

Benefits

The Maestro debit program has many benefits:

*   PIN debit gives you a competitive advantage by offering an option to your customers that grows faster than any other payment means.

*   Offers the ability to provide over 654 million[3] Maestro card users worldwide hassle-free access to their checking accounts

*   Reduces your risk of bounced checks and disputes as debit transactions are completely electronic

*   Reduces your fraud risk and chargeback events because every transaction is authenticated by the customer

*   Reduces check processing and collection costs, along with your Non Sufficient Funds (NSF) risk, when customers use their Maestro cards instead of checks

*   Reduces your float from out-of-region checks

*   Extends your reach to customers worldwide as the Maestro brand spans your geographic coverage in each of your trading areas

For more information about the Maestro debit program, contact your acquirer or MSP.

Co-branded MasterCard Cards

Co-branding is a partnership between MasterCard, your business, and issuer that can result in increased card usage, higher spending levels, efficient marketing opportunities, and higher satisfaction and value for customers.

Co-branded cards are designed with your company brand as the dominant brand represented on the card, but also contain the MasterCard logo and hologram, as well as the name of the issuer.

---

3.   Figure as of September 2010.

Co-branding can help to elevate your brand in your customers' minds and increase the frequency of their visits by offering attractive incentives. A co-branded MasterCard card gives your customers the opportunity to participate in rewards programs. Monthly statements let you reach out to your customer base regularly. You can then strengthen retention and loyalty through promotions, cross-selling opportunities, frequent-buyer programs, rebates, and other incentives.

NOTE

MasterCard is not an issuer.

Benefits

Co-branded MasterCard cards provide the following benefits:[4]
- Co-branded cardholders outspend their counterparts by approximately USD 4,900 per year
- Co-branded credit cards comprise 55 percent of all credit card spending
- Co-branded cards drive usage and preference as consumers seek to "get something back" for their business and loyalty
- Co-branded card spend is growing at a faster rate than that of non–co-branded cards

Implementation

For many businesses, co-branding is an excellent way to take their businesses to the next level. To help you get started, answer the following questions:
- Do you have a significant database of customers?
- Does your business engender loyalty and repeat customer transactions?
- Is there something that makes your company distinctive and differentiates it from your competition?
- Do you offer a range of products and services?
- Do you anticipate strong growth trends for your business or your industry as a whole?
- Would a customer points/reward program be appropriate for your business?

If the answer to most of these questions is "yes," you should consider a co-branded card program. If you're not sure, call the Co-brand Help line in the U.S. at 1-800-299-9408 to speak to a Co-brand Specialist.

MasterCard can help you determine if a co-brand program is right for your business. MasterCard also remains a key part of your co-brand alliance, working with you and your selected partner. From business plan development to identifying benefits relevant to your customers, to communicating your ideas to your issuer, MasterCard can help ensure that your program goals are realized.

---

4. Sources: Nilson Reports, First Annapolis Consulting, Boston Consulting Group. The data set forth above in this study derived from information provided to MasterCard and is subject to certain limited verification by MasterCard. Certain information indicated on the study may not have been independently verified by MasterCard. All data is subject to revision and amendment by MasterCard subsequent to the date of the release of this study.

Prepaid Cards

Consumers want a convenient and simple method of payment. By accepting and selling MasterCard prepaid cards, you'll not only give your customers that, but you'll open your business to an ever-widening population of prepaid cardholders—from gift-givers, travelers, corporate and public sector employees, to those who don't have access to traditional banking services.

MasterCard prepaid cards allow you to enter new market segments, create new customer relationships, help generate more revenue, and help grow your business. U.S. consumers are projected to spend over $86 billion in 2017 using Consumer Prepaid products including gift, travel, and everyday prepaid cards. Globally, consumer spend estimate is $274 billion in 2017.[5]

Prepaid card usage is also growing in the commercial and public sector categories, which include public benefit and welfare programs, pension and Social Security, corporate gift and incentive, payroll, and healthcare segments. In fact, the projected total amount spent using open loop prepaid cards is expected to top $840 billion globally in 2017.

Types of Prepaid Cards

The following information describes the various types of prepaid cards.

- **Everyday Prepaid Cards**—An affordable and effective way for consumers who don't have basic banking services to shop, pay bills, and manage spending effectively. They're easy to get and easy to use with no credit check required, and they're accepted everywhere Debit MasterCard® is accepted. If the card is lost or stolen, cardholders are protected from unauthorized purchases with MasterCard® Zero Liability[6]. In addition, cardholders can have their paychecks directly deposited to their Everyday Prepaid Card to make paying bills and managing expenses easier.

- **Prepaid Gift Cards**—Make choosing the perfect gift easier for your customers. Most people prefer a prepaid gift card to a traditional gift of equal value. In fact, 4 out of 5 consumers prefer a $100 gift card over a traditional gift of the same value.[7]

- **Travel Cards**—The safe and convenient alternative to cash and travelers' checks, they are accepted at millions of locations worldwide, wherever MasterCard cards are accepted. If the cards are lost or stolen, cardholders are protected from unauthorized purchases with Zero Liability. In addition, cardholders are also protected with the emergency cash advance or card replacement feature

- **MasterCard Prepaid Payroll Card**—A cost-effective way to pay employees who don't have access to traditional banking services.

---

5. Source: Prepaid Market Assessment, Boston Consulting Group, May 2010. Research commissioned by MasterCard.

6. Card registration required. Certain exceptions apply.

7. Source: MasterCard Prepaid Gift Card Survey – Quantitative Research Report, November 2005.

The MasterCard® *rePower*™ Load network is a service that enables consumers to add money to eligible MasterCard or Maestro® prepaid cards at any of the thousands of participating retailer locations throughout the U.S. To find a location, go to www.mastercard.com/repower.

For more information about MasterCard prepaid cards and MasterCard business prepaid cards , visit www.mastercard.com/us/merchant.

Merchant Rules and Responsibilities

The MasterCard Worldwide Network operates under a specific set of Standards that inform, guide, and provide clarity to all of its members, processors, and merchants. As a MasterCard merchant, you have access to and should understand applicable MasterCard Standards.

MasterCard requires our members to comply with MasterCard Standards. Those members must ensure that their processors and the merchants they acquire for also comply with MasterCard rules.

MasterCard has made the rules for the MasterCard and Maestro brands available to merchants at www.mastercard.com/us/merchant. Please note that MasterCard Standards change frequently. While MasterCard strives to keep these documents up to date, it is possible that they will not always be absolutely current in all regards. In the event of any discrepancy between the documents provided to merchants online and Standards MasterCard deems to be current and in effect, the Standards deemed current and in effect by MasterCard will apply.

For the rules governing the MasterCard family of brands or when you need information about MasterCard acceptance, refer to the following documents:

- *Chargeback Guide*
- *Maestro Global Rules*
- *MasterCard Rules*

Security Rules and Procedures—Merchant Edition

The *Security Rules and Procedures—Merchant Edition* addresses certain responsibilities of a MasterCard member, particularly those regarding any merchant from which the member acquires MasterCard and Maestro transactions. Portions of the *Security Rules and Procedures—Merchant Edition* manual included in the Merchant Edition address certain responsibilities of a MasterCard member, particularly those regarding any merchant from which the member acquires MasterCard transactions. The included portions also describe programs that MasterCard administers, such as merchant audit, monitoring, and registration to ensure that its members and merchants are acting in an appropriate fashion so as to protect cardholder information and reduce chargebacks and fraud.

For additional information, see *MasterCard Rules* and *Maestro Global Rules.*

What You Can't Do

MasterCard prohibits merchants from engaging in the following practices. For more detailed information about prohibited practices, refer to *Chargeback Guide*, *Maestro Global Rules*, and *MasterCard Rules*.

- **Discrimination**—A merchant must not engage in any acceptance practice that discriminates against or discourages the use of a card in favor of any other acceptance brand.

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

- **Minimum or maximum transaction amount prohibited**—A merchant must not require, or indicate that it requires, a minimum or maximum transaction amount to accept a valid and properly presented card. A merchant located in the U.S. may set a minimum transaction amount (not less than USD 10) to accept MasterCard cards that access a credit account. Merchants in the U.S. that are a department, agency, or instrumentality of the U.S. Government or a corporation owned or controlled by the U.S. Government or a merchant located in the U.S. that falls under the following MCCs may set a maximum transaction amount to accept MasterCard cards that access a credit account:

  - MCC 8220—Colleges, Universities, Professional Schools, and Junior Colleges

  - MCC 8244—Schools, Business and Secretarial

  - MCC 8249—Schools, Trade and Vocational

- **Scrip-dispensing terminals**—Cards must not be accepted at terminals that dispense scrip.

- **Prohibited transactions**—A merchant must not submit for payment into interchange, and a member must not accept from a merchant for submission into interchange, any transaction that represents the refinancing or transfer of an existing cardholder obligation that is deemed to be uncollectible, or arises from the dishonor of a cardholder's personal check, or arises from the acceptance of a card at a terminal that dispenses scrip.

- **Other forms of payment**—A merchant must not accept any payment from a customer in any other form (for example, cash or check) with respect to a charge for products or services reflected on a transaction information document (TID) resulting from the use of a card. A merchant also must not accept a card as payment for products or services for which the merchant has received or expects to receive payment in any other form, whether from the customer or a third party.

Frequently Asked Questions

The following information may help answer general merchant questions about card acceptance. If your question is not here, please contact your acquirer or MSP.

I am having trouble getting an account to accept MasterCard cards. What should I do?—Many acquirers and MSPs have firm guidelines as to what types of businesses they can support and how much risk they can manage. It pays for you to shop around for service or for information that may be helpful in matching your needs with an acquirer or MSP's interest, see How to Accept MasterCard Cards.

How can I get involved in electronic commerce?—Many acquirers and MSPs can assist you in accepting cards over the Internet or by mobile phone. In fact, many can help you create a Web site, add a shopping cart function, and enhance the security of your site and transactions. For more information about getting involved in electronic commerce, contact your acquirer or MSP.

What is a Smart Card, and how can this new technology help my business?—The Smart Card is a card embedded with a computer chip. Smart Cards are simple to use and to accept, and they can give cardholders increased convenience and control. These cards can remember past card activity and keep track of purchases—offering merchants and acquirers and MSPs many marketing opportunities.

How can I direct my customers to the closest ATM that will let them get cash with their MasterCard card?—MasterCard cardholders have access to more than a million automated teller machines all over the world. To find the locations nearest you or to download an ATM Hunter iphone application, go to the MasterCard Global ATM Locator Web page.

What should I do if my customers need a replacement card?—Direct your customers to call MasterCard Global Service®. One call offers cardholders the security of worldwide emergency assistance in their own languages, 24 hours a day, 365 days a year, from anywhere in the world. In the U.S., call 1-800-MCASSIST.

What is the procedure when a card is presented but cannot be swiped?—The merchant should manually enter the card in the POS device, as well as take an imprint of the card and have the cardholder sign the imprinted copy

How can I download the MasterCard brand mark for use on my Web site?—Electronic versions of the MasterCard Brand Mark are available from the MasterCard Brand Center for download.

Chapter 4 Transaction Processing

This chapter provides an overview of how MasterCard transactions are submitted. Information about MasterCard systems and the participants in a typical transaction is also included.

Participants in Transaction Processing

In transaction processing, there are several participants in a typical transaction.

Cardholder

A cardholder is a person to whom a card has been issued or a person who is authorized to use the card. In an authorization transaction, the cardholder presents the card or cardholder account number as payment in exchange for goods or services.

Merchant

A merchant is a commercial entity or person that pursuant to a merchant agreement is authorized to accept cards and access devices when properly presented. The merchant is a retailer, or any other person, firm, or corporation that (pursuant to a merchant agreement) agrees to accept credit cards, debit cards, or both, when properly presented.

Acquirer

An acquirer (merchant bank) is a licensed MasterCard member that acquires the data relating to a transaction from the merchant and submits that data for authorization. The acquirer also supports clearing and settlement functions to exchange funds between the issuer and the merchant.

Issuer

An issuer (card issuer) is a licensed MasterCard member that issues cards or access devices to accountholders. Issuers are responsible for approving or declining authorization requests. The issuer also bills cardholders and supports clearing and settlement functions to exchange funds between the cardholder and the acquirer.

NOTE

MasterCard is not an issuer.

Anatomy of a MasterCard Transaction

The following illustrations show the four steps of a transaction process.

1. TRANSACTION BEGINS
The cardholder purchases goods or services from the merchant.

2. AUTHENTICATION
The merchant, in effect, sells the transaction to the "acquirer" and is reimbursed the amount of the sales ticket less a "discount fee."
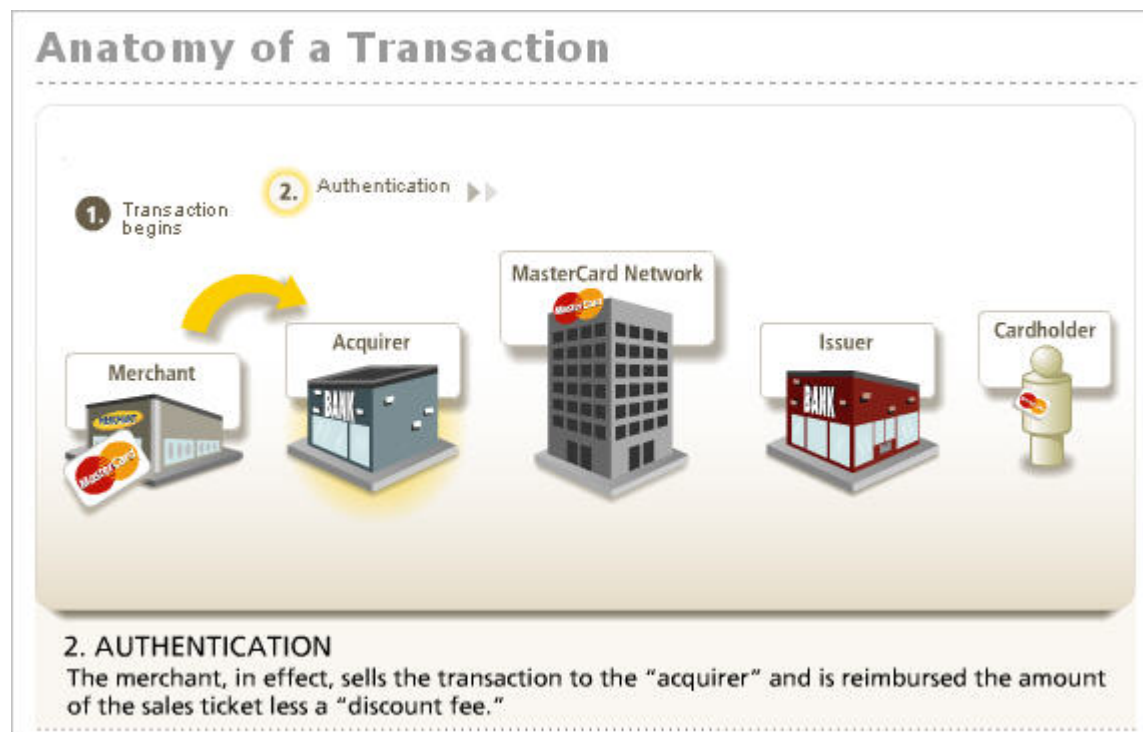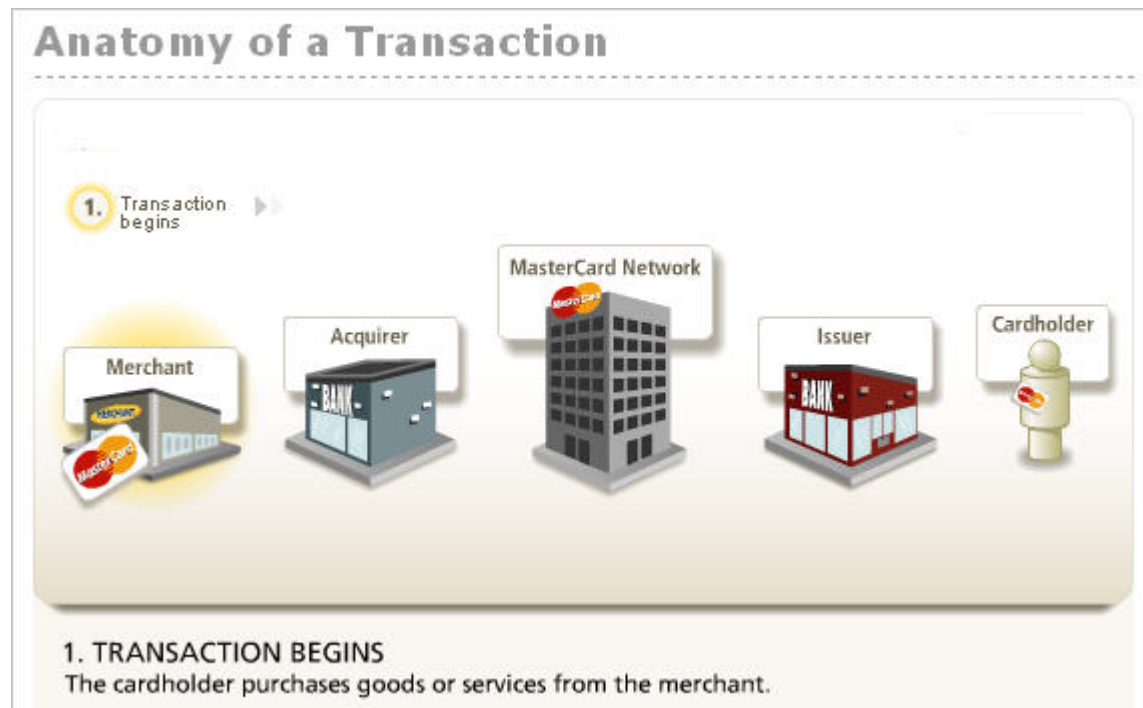
Anatomy of a Transaction
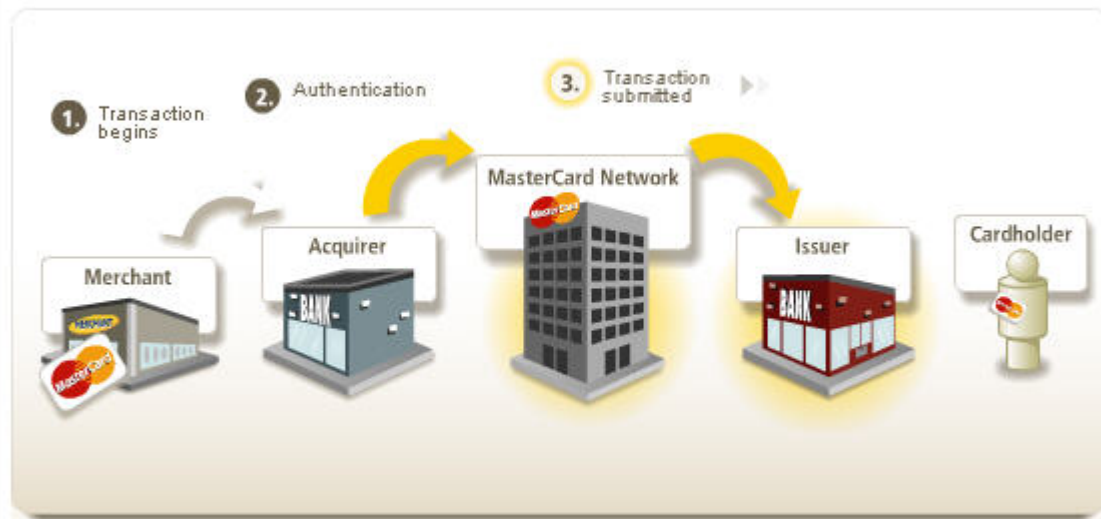
3. TRANSACTION SUBMITTED
The acquirer then submits the transaction to the issuing bank for payment via the MasterCard interchange and settlement system.

Anatomy of a Transaction
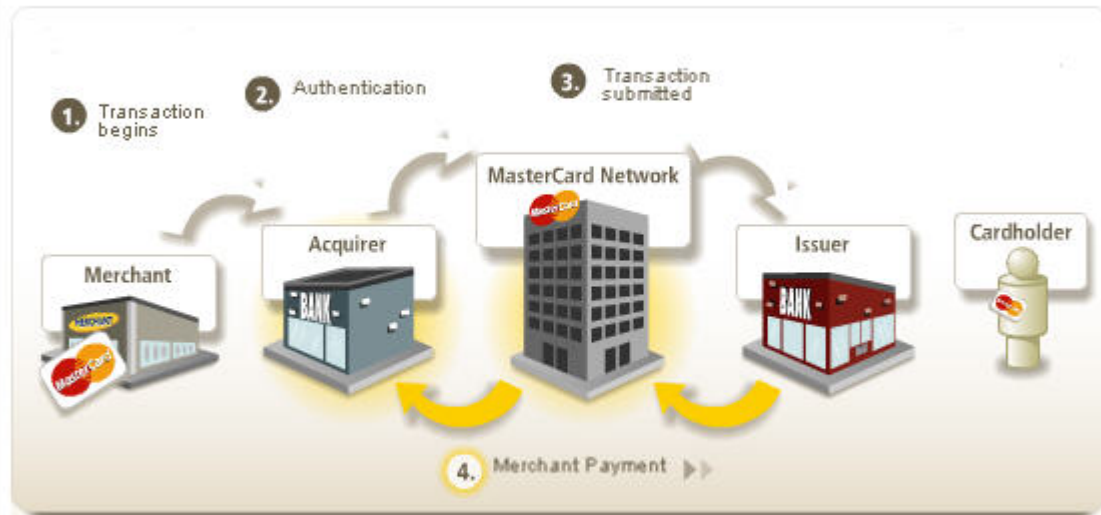
4. MERCHANT PAYMENT
The issuing bank pays the merchant acquirer, less an interchange fee which partially reimburses the issuer for its expense, through the MasterCard settlement system.

Authorization, Clearing, and Settlement Processing

MasterCard dual message transactions are processed through the MasterCard Worldwide Network using the Authorization Platform, Global Clearing Management System (GCMS), and the MasterCard Settlement Account Management (S.A.M.) system.

Authorization Platform

The Authorization Platform approves payment card transactions and performs Stand-In authorizations on behalf of issuers.
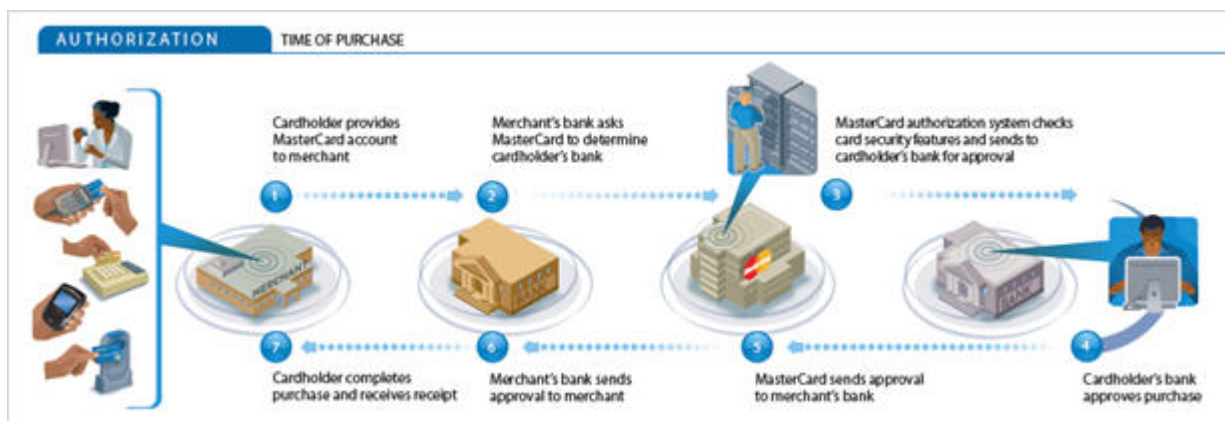
Global Clearing Management System

GCMS, which is a centralized clearing facility owned and operated by MasterCard, performs daily processing and routing of financial transactions between MasterCard and its acquirers and issuers.
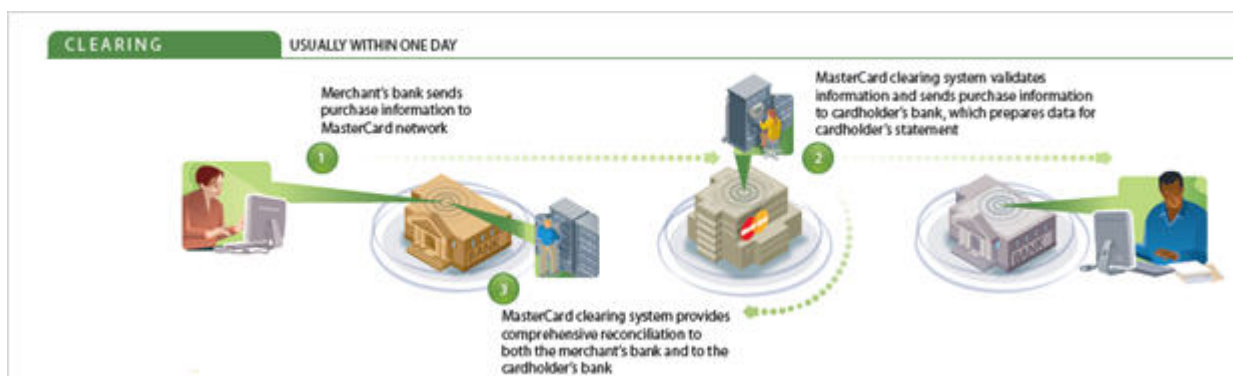
Settlement Account Management

The S.A.M. system generates advisements and funds transfer for the purpose of the financial settlement of clearing transactions, MasterCard fees, and other transfer of funds between MasterCard and its acquirers and issuers.
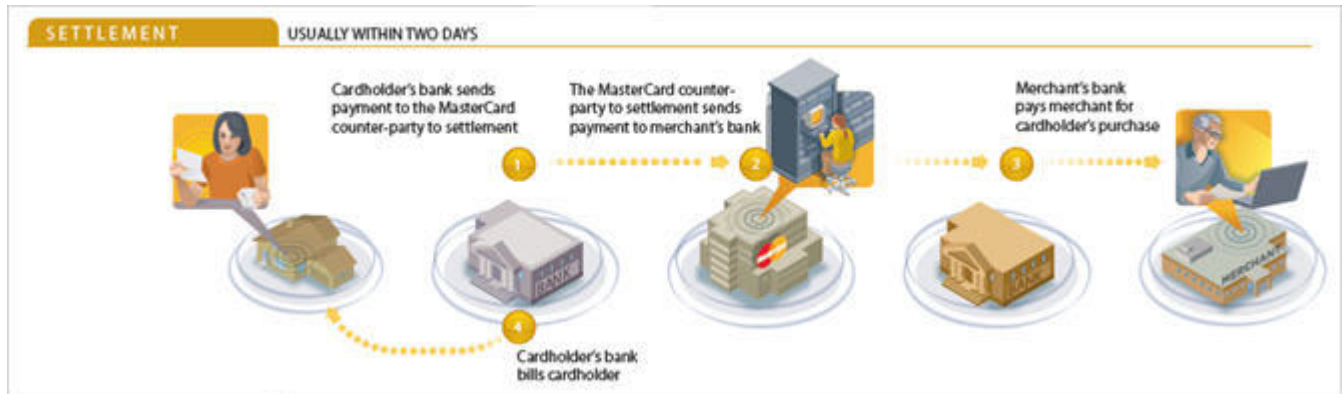
Authorization

Every authorization request receives an authorization response that directs the acquirer or the merchant on how to proceed with the transaction. The response received is typically a code that identifies the action that the merchant should take. The format of the authorization response depends on the acquirer's access method.

If the acquirer is online, the authorization request response message includes a two-digit response code. This code informs the acquirer and merchant of the action to be taken (approve, decline, refer to card issuer, capture card, or valid).

Regardless of the format in which the authorization response is received, the response always prompts one of the following actions on the part of the merchant.

Response	Description
Approve	The transaction is authorized as reported.
	For magnetic stripe, chip, and key-entered transactions, the issuer provides a six-digit authorization code to the acquirer when it approves a transaction for the purchase of goods or services or cash disbursement.
	The merchant still must perform its normal review process (steps such as verifying the signature on the card are often included) before completing the transaction.
Decline	The merchant may not complete the transaction. The merchant may return the card but may not accept the card in payment for the program or service for that transaction amount.

Response	Description
Refer to card issuer	The acquirer or merchant must contact the issuer for further instructions.
Capture card	The acquirer or merchant must use its best efforts to retain the card by reasonable and peaceful means.
Valid	Not declined—used for inquiry transaction types only.
	Issuers provide a valid response when processing balance inquiries, address verification requests, or other non-financial types of requests. The valid response indicates to the acquirer or merchant that the request was completed successfully by the issuer, that is, the balance returned, address verification response information provided, and so on. Merchants use the information returned in the response message to provide information to the cardholder or to determine if further authorization decisioning is required.

When a cardholder uses a MasterCard® card to purchase goods or services from a merchant, the acquirer reimburses the merchant for the transaction. The acquirer then settles those funds with the issuer by presenting the transaction into interchange. MasterCard provides this functionality.

Partial Approvals

The partial approval enables merchants and cardholders to successfully complete a higher percentage of debit card (including prepaid) purchases and reduce checkout time when the cardholder uses a debit card (including prepaid) with an available balance that is less than the transaction amount.

The partial approval enables an issuer to approve a portion of the transaction amount in the authorization request when the transaction amount exceeds the amount of funds available on the debit card or prepaid card and the merchant terminal supports partial approvals. For automated fuel dispensers (AFDs), an issuer may respond with a partial approval amount that is greater than the amount provided in the authorization request.

When the acquirer transmits an indicator in the authorization request that the merchant terminal supports partial approvals, the issuer has the option to respond with the partial approval amount and partial approval response code. The cardholder can then choose to use a supplemental payment method (split tender) to pay the balance and complete the purchase.

All Debit MasterCard® card issuers (including prepaid) in the U.S. region must support partial approvals and updates to the cardholder's open-to-buy balance upon receipt of a reversal (full or partial).

All acquirers in the U.S. region that support merchants within select card acceptor business codes (MCCs) must support partial approvals for all Debit MasterCard® account ranges, including all prepaid Debit MasterCard account ranges. This requirement applies only to card-present transactions occurring at attended terminals and at cardholder-activated terminals (CATs) identified with MCC 5542 (Fuel Dispenser, Automated). For effective dates for acquirers in the U.S. region to begin supporting partial approvals, full and partial reversals, and account balance responses by MCC, refer to Rule 3.8.4 in the *MasterCard Rules*.

Upon receipt of a partial approval, acquirers often send a balance due message to the integrated terminal. This message indicates the difference between the original purchase amount and the partial amount approved by the issuer. By displaying the remaining balance due amount, the merchant can quickly and accurately prompt the customer to complete the split-tender purchase.

Clearing

Acquirers and issuers perform clearing to exchange transaction data. From the data provided in clearing, the MasterCard Global Clearing Management System (GCMS) derives the amounts for settlement. Members that issue MasterCard® cards and acquirers contracting with merchants to accept cards must perform clearing to exchange transaction data.

Clearing is the process of exchanging clearing data. For example, clearing includes sending transactions from the acquirer to the issuer for posting to the cardholder account (also called "presentment"). GCMS accepts the data, edits it, assesses the appropriate fees, and routes it to the appropriate receiver. The clearing messages contain data but do not actually exchange or transfer funds.

GCMS manages the clearing processing of credit transactions and debit transactions (in offline mode). GCMS is a centralized clearing facility owned and operated by MasterCard for the daily processing and routing of worldwide financial transactions between MasterCard and its members.

Settlement

Settlement is the process by which funds are exchanged. The funds represent the net equivalent of monetary value from clearing processing. These funds are exchanged each day between acquirers and issuers for the net monetary value of the cleared transactions.

MasterCard calculates in reconciliation currency the net position of each acquirer and issuer involved in the clearing process and performs the following two settlement functions:

- Sending advisements
- Transferring funds (when applicable)

Chapter 5 Card Security

This chapter provides information about card security requirements and recommendations, security and card verification programs, and MasterCard card identification features.

Overview

MasterCard is committed to bringing advanced, innovative security solutions and working with leading security experts to protect your business and your customers.

Requirements and Recommendations

Merchants must follow specific data security requirements to accept MasterCard® cards. MasterCard rules and recommendations apply to all transactions—whether they occur in a store, online, or over the phone.

- **Make Sure Your Systems Are Secure**—The systems you use to accept MasterCard payment cards in your store or business must comply with industry-mandated security requirements and with the Payment Card Industry (PCI) Data Security Standard.
- **Be Fraud Savvy**—The three main types of card fraud are altered/counterfeit cards, lost/stolen cards, and Card Not Present fraud. You can help protect your business from fraudulent use of payment cards by:
  – Incorporating fraud prevention into employee training sessions
  – Posting fraud prevention reminders and materials near registers and in employee areas
  – Offering rewards or incentives for employees who prevent a fraudulent transaction
- **Stay Informed**—MasterCard continues to develop new ways to protect your bottom line. Stay informed on the latest security programs and techniques and payment card enhancements.
- **Make Remote Shopping More Secure**—For online shoppers, MasterCard offers OneSMART® Authentication, a chip-based solution that uses a card reader to generate one-time passwords for highly secure shopping over the Internet. The same approach can be used to secure mail or telephone order payments, and remote banking transactions.

  MasterCard *SecureCode*™ also is designed to help merchants and issuers make Internet transactions more secure.

Security Programs, Techniques, and Payment Card Enhancements

MasterCard supports the following security programs, techniques, and payment card enhancements.

MasterCard Site Data Protection Program

The MasterCard Site Data Protection™ program is deployed globally by MasterCard and consists of a combination of rules, guidelines, best practices, and approved compliance validation tools to foster broad compliance with the PCI Data Security Standard.

MasterCard requires issuers, acquirers, merchants, and third-party processors to comply with PCI Data Security Standard. Entities handling payment cards can work to achieve compliance with PCI Data Security Standard using the MasterCard Site Data Protection Program. This program applies to merchants and member service providers (MSPs) that process, transmit, or store cardholder data. Through the network scanning requirement, this program is also designed to protect against the compromise of account data. Remember that your acquirer should be closely monitoring your compliance with PCI Data Security Standard.

With PCI Data Security Standard as the foundation, the MasterCard Site Data Protection program details data security requirements, compliance validation requirements to protect stored and transmitted MasterCard account information, and identifies vulnerabilities in security processes, procedures, and Web site configurations. Adoption of the MasterCard Site Data Protection program and subsequent compliance with the PCI Data Security Standard help merchants, MSPs, and acquirers protect against security breaches, enhance consumer confidence, and protect the integrity of the overall payment channel.

Choosing a Trusted Vendor

MasterCard requires merchants to demonstrate compliance with the PCI Data Security Standard. An approved scanning vendor will evaluate your Internet-facing environment to find vulnerabilities and offer guidance on how to fix them. If you require an on-site assessment, a qualified security assessor can validate your adherence to the PCI Data Security Standard.

For More Information

For more information about:

* Payment Card Industry Data Security Standard, go to www.pcisecuritystandards.org/security_standards/pci_dss.shtml

* MasterCard Site Data Protection Program, go to www.mastercard.com/us/sdp/index.html

For a list of approved scanning vendors and qualified security assessors, go to www.pcisecuritystandards.org/qsa_asv/find_one.shtml

Quick Payment Service

Consumers are using cash less often than they did five years ago. To make the "cashless" trend work for merchants, even for low-value payments, MasterCard introduced the Quick Payment Service. For purchases under certain currency amounts, signatures are no longer required by qualified merchants (to preserve chargeback rights). This added customer convenience saves time at the point of sale. Shorter lines and increased efficiency at the checkout counter are likely to result in greater sales, without increasing costs for security.

The Quick Payment Service applies to all face-to-face card acceptor business codes (MCCs), excluding Unique transactions.

If your business depends on moving customers quickly through checkout, you can benefit from QPS. For more information about QPS and the regional variations of the program, see the *Quick Payment Service Program Guide* and Appendix C of the *Chargeback Guide.*

MasterCard *PayPass*

MasterCard® *PayPass*™ adds an embedded radio frequency chip and antenna to MasterCard cards or new contactless devices. With *PayPass*, consumers speed through checkout with a simple tap, rather than a swipe or a dip of their card. When combined with the MasterCard QPS program, no signature is necessary for many purchases under certain currency amounts, so consumers just Tap & Go™.

As *PayPass* cards and devices never leave their hands, cardholders have an added sense of security. Advanced chip-based cryptography (CVC 3) delivers another layer of security to make this fast and convenient payment a safe option as well.

Types of Merchants that Benefit Most from MasterCard *PayPass*

PayPass is ideal for traditional, cash-only environments where speed is essential, such as fast-food restaurants, drive-thrus, convenience stores, movie theaters, self-serve gas stations, mass transit, pharmacies, parking garages, and toll roads. The most significant time savings were recognized at drive-thrus where *PayPass* saved between 12 and 18 seconds from the purchase time, as compared to cash.

MasterCard *PayPass* Vendors

Numerous vendors develop products and services for *PayPass*. For a current list, go to www.paypass.com.

Chip Technology

Payment cards containing chips are more powerful than traditional magnetic stripe cards because they contain tiny computers that allow for additional chip-enabled capabilities. Chip technology also reduces the incidence of fraud by making cards more difficult to counterfeit. Although chip technology is widely used in some areas of the world, it is still emerging in other areas.

Internet Protocols and Wireless Technologies

Internet Protocols (IP) communications and wireless technologies are revolutionizing the point of sale (POS). They provide fast, flexible and low cost solutions to connect stand-alone POS terminals to networks and acquirers. However IP enabled or wireless-enabled stand alone POS terminals can be subject to cyber theft.

Point-of-Sale Terminal Security Program

The security evaluation program for IP-enabled POS devices ensures the necessary level of protection for transaction and cardholder data at merchants that use equipment that support the TCP/IP protocol suite. The security evaluation verifies that POS devices meet the relevant MasterCard requirements in terms of confidentiality, integrity, and communicating parties' authentication. By addressing the interface of POS terminals to open networks using open protocols, this security program complements existing security programs at MasterCard that already address merchants or POS, such as PCI POS PED (security of PIN provided by PIN Entry Devices) and SDP (based on the PCI Data Security Standard).

For a list of approved POS terminals and description of the PTS program, refer to the *POS Terminal Security Program—Approval List.* Any queries related to the PTS program or the encryption requirements can be sent to pts@mastercard.com

Card Verification Programs

MasterCard recommends using the following programs to make transactions safer and more profitable.

Address Verification Service

The Address Verification Service (AVS) is a mandatory service for issuers in the U.S. It is optional in the rest of the world; and, as such, it is mostly used in Canada, the U.K., and the U.S. AVS is a fraud deterrent service that provides greater security to merchants and cardholders. It helps to protect against fraudulent use of cards in non–face-to-face transactions by allowing issuers to verify the cardholder's billing address.

When a customer provides an address with an order, AVS automatically compares it to the billing address on file with the issuer. This risk reduction measure is especially helpful to merchants conducting business on the Internet. If the billing address and the card address on file do not match, you will receive a response code indicating this during transaction processing. A merchant can then choose to either deny the transaction or proceed with the transaction.

The acquirer requests the cardholder billing address verification as part of the authorization request message or uses an authorization request to request address verification only. The issuer performs the verification and returns the appropriate information to the acquirer in the authorization request response message.

For more information about AVS, contact your acquirer or member service provider (MSP).

Card Validation Code 2 Verification

Card validation code 2 (CVC 2) verification provides added security for the card authentication process for authorization requests in non–face-to-face environments.

CVC 2 is a three-digit code algorithmically derived by the issuer and is present in a white panel adjacent to the signature panel and to the right of the last four digits of the MasterCard account number, which are present in the upper right corner of the signature panel. CVC 2 is one of several card authentication methods currently used by MasterCard to combat fraud. The use of CVC 2 deters fraudulent use of an account number for non–face-to-face transactions.

MasterCard strongly recommends that businesses ask each consumer for the CVC 2 when conducting a transaction on the Internet or by phone. Merchants must never store CVC 2 codes.

For more information about CVC 2, contact your acquirer or MSP.

Electronic Commerce

Electronic commerce (e-commerce) transactions are non–face-to-face, online transactions that use electronic media over any public network such as the Internet, or private network such as an extranet. E-commerce processing allows transactions to be initiated from a cardholder-controlled device, such as a PC, for purchasing goods and services on the Internet.

Process for an Electronic Commerce Transaction

A typical e-commerce transaction follows this process:
1. The cardholder accesses a merchant's Web site via the Internet and requests to make a purchase.
2. The merchant submits the cardholder's information to the acquirer.
3. The acquirer sends an authorization request message through the MasterCard authorization network to the issuer.
4. The issuer makes the authorization decision and replies using an authorization request response message.
5. The acquirer responds to the merchant.
6. The merchant completes the transaction according to the authorization response returned.

Security of Electronic Commerce Transactions

MasterCard messaging requirements regarding e-commerce may vary depending on the security protocol involved in the transactions. Security protocols may include:
- No security protocol
- Channel encryption, which is a security layer that resides between an application and its transport layers, for example, SSL (Secure Sockets Layer) and HTTPS (Hypertext Transfer Protocol Secure)

- *SecureCode* transaction using the Universal Cardholder Authentication Field (UCAF™)

MasterCard *SecureCode*

MasterCard® *SecureCode*™ is designed to help merchants and issuers make Internet transactions more secure.

SecureCode is a global e-commerce solution that:

- Enables cardholders to authenticate themselves to their issuer through the use of a unique personal code.

- Addresses current consumer concerns about the security of online shopping and the higher rate of e-commerce chargebacks compared to face-to-face transactions.

- Builds on the infrastructure requirements for channel encryption with the additional benefit of cardholder authentication. When used in conjunction with components of the MasterCard payment infrastructure, this program provides a mechanism for online merchants to potentially receive chargeback protection similar to what merchants (non-Internet) receive with qualifying physical point-of-sale transactions.

- Takes online shopping security and consumer confidence to a new level.

Why Use *SecureCode*

Once the merchant has enabled *SecureCode*, the issuer authenticates its cardholders for online transactions. The authentication data, together with an authorization approval, gives the merchant a transaction that is guaranteed against the most common types of chargebacks—"cardholder not authorized" and "cardholder not recognized" chargebacks.

Similar to an ATM authentication process, cardholders enter their *SecureCode* in an issuer-provided window before their online transaction can be authorized. In seconds, the issuer validates the personal code and approves the transaction. Cardholders enjoy peace of mind knowing that no one else has access to their *SecureCode*. The participating merchant gets explicit evidence of an authorized purchase (authentication data) with minimal cost impact and time investment.

SecureCode requires that 3-D Secure technology be enabled on the merchant Web site. This can be done by loading a *SecureCode*-compliant merchant plug-in application on your server or by contracting with a hosted service to perform the authentication process for you. Merchants should then work with their acquirer or MSP to pass authentication data via the MasterCard Universal Cardholder Authentication Field (UCAF™), a simple, common method of collecting and passing cardholder authentication data at the merchant Web site. This data transport mechanism standardizes how cardholder data is carried among all parties in a transaction—cardholders, merchants, issuers, and acquirers.

SecureCode also supports Maestro® cards. *SecureCode* provides a way for issuers to support Maestro debit transactions over the Internet. This allows more cross-border transactions with merchants in countries where debit is more established than credit. *SecureCode* is required for merchants that want to accept Maestro e-commerce transactions.

Authorization Requests

MasterCard requires authorization requests for MasterCard Electronic™ cards acquired in e-commerce environments to be fully authenticated through *SecureCode*. MasterCard Electronic issuers that want to process e-commerce transactions must participate in *SecureCode* and provide UCAF™ data for e-commerce transactions for a MasterCard Electronic card. MasterCard Electronic acquirers and merchants that want to process e-commerce transactions must participate in *SecureCode* and be UCAF enabled.

To Participate

Contact your acquirer or MSP to confirm that they support the MasterCard *SecureCode* program. If they do not, send an e-mail to securecodemerchant@mastercard.com. For more information about becoming a *SecureCode* merchant, go to www.securecodemerchant.com.

MasterCard Data Security Rules

The *Security Rules and Procedures—Merchant Edition* addresses certain responsibilities of a MasterCard member, particularly those regarding any merchant from which the member acquires MasterCard transactions. The included portions in the *Security Rules and Procedures—Merchant Edition* also describe programs that MasterCard administers, such as merchant audit, monitoring, and registration to ensure that its members and merchants are acting in an appropriate fashion so as to protect cardholder information and reduce chargebacks and fraud.

For additional information, see *MasterCard Rules* and *Maestro Global Rules*.

MasterCard Card Identification Features

All MasterCard cards have security features for merchants to check during a transaction. If you are ever suspicious about the validity of a MasterCard card, call your Voice Authorization Center and request a Code 10.

A Code 10 authorization request alerts the issuer to suspicious activity—without alerting the customer. During a Code 10 call, your acquirer may ask for transaction details. Your staff will be transferred to the issuer's special operator who will provide instructions on any necessary action.

The following illustration shows MasterCard® card security features and optional card features.

NOTE

Maestro card design standards will differ from MasterCard card design standards. For more information about Maestro card designs, visit the MasterCard Brand Center.

Card Front

Card Feature	Description
1	The first 4 digits of the account number must match the 4 digit preprinted BIN. Remember that all MasterCard account numbers start with the number 5.
2	The last 4 digits of the account number must match the 4 digits that appear on the cardholder receipt.
3	The global hologram is three dimensional with a repeat "MasterCard" printed in the background. When rotated, the hologram will reflect light and appear to move.
4	The stylized "MC" security feature has been discontinued but may continue to appear on cards through 1 June 2010.

Card Back
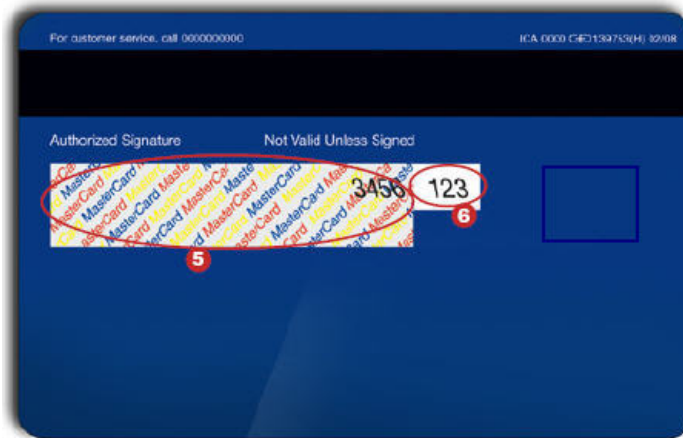
Card Feature	Description
5	The signature panel is tamper-evident with the word "MasterCard" printed in multiple colors at a 45º angle. For magnetic swiped transactions, remember to compare the signature on the back of the card with the cardholder's signature on the receipt.
6	The 4 digits printed on the signature panel must match the last 4 digits of the account number, followed by the 3-digit CVC 2 number.

Optional Card Features

The following card features on the front of the card are optional.

Card Feature	Description
7	Chip may be present on the card. The cardholder may be prompted to enter a unique personal identification number or PIN when the card is inserted into a chip-capable payment terminal.
8	*PayPass*® contactless payment technology may be present on card.
	A signature is not required for *PayPass*® "tapped" transactions below certain currency amounts.

Other Optional Card Design Features

Other optional card design features that MasterCard offers issuers include flexible placement of the MasterCard hologram (card front or back), may permit the use of holographic magnetic tape, and supports vertical card designs.

Card Front

Card design and MasterCard brand mark may be oriented vertically.
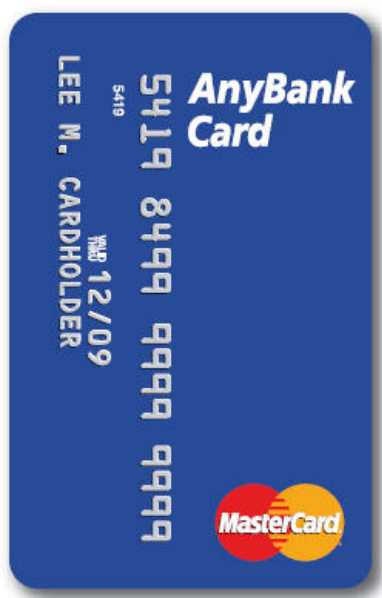
Card Back

Global hologram on the back of a chip card design. The signature panel has been shortened to accommodate the chip.

Debit Hologram on the back of a magnetic stripe card design of a non-chip card.

NOTE

In some countries, it is mandatory for Debit MasterCard cards to bear the Debit hologram.
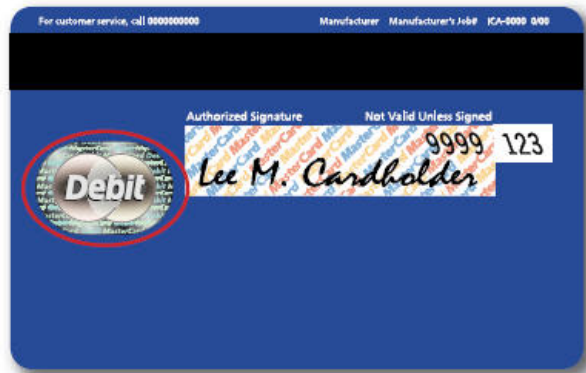
Holographic magnetic tape may be used in lieu of the hologram or in conjunction with the hologram. A longer signature panel is used on traditional magnetic stripe cards when the MasterCard Brand Mark and hologram appear on the card front.
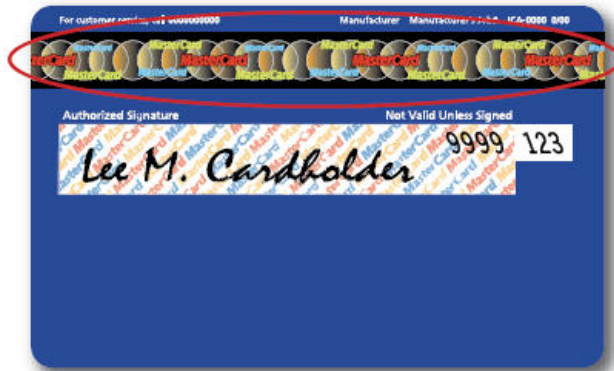
Chapter 6 Interchange

This chapter explains interchange and interchange rates established by MasterCard.

Overview

Interchange rates and fees are established by MasterCard and are generally paid by acquirers that provide card acceptance services to merchants. Acquirers pay these fees to issuers. Interchange rates/fees are only one of the many cost components of the Merchant Discount Rate (MDR) that is established by acquirers and paid by merchants in exchange for card acceptance services.

As a MasterCard merchant, it's important for you to know the economic model that underlies payment card transactions. Although MasterCard interchange rates have generally been available to merchants by request to acquirers and other card acceptance providers, MasterCard wants the process to be as transparent as possible; therefore, MasterCard publishes interchange rates and related criteria on the merchant Web site (www.mastercardmerchant.com). While MasterCard will endeavor to keep the rates and related criteria on the Web site up to date, it is possible that this Web site will not be absolutely current in all regards. In the event of any discrepancy between the rates and criteria found in this document and those rates and criteria MasterCard deems to be the official rates and criteria, the official rates and criteria will apply.

Every business establishes a price for the goods and services it provides, and the electronic payments business is no exception. As one element of the cost of acceptance, interchange is a small fee in relation to the enormous value merchants receive for accepting MasterCard payment cards.

MasterCard has established default interchange fees that have proven to be the most efficient way to balance costs in the system and to promote a strong, competitive payments industry that benefits cardholders, merchants, and financial institutions. Financial institutions provide the cards and services that allow consumers and merchants worldwide to benefit from the convenience and security of electronic payments.

What is Interchange

Interchange is established to incent banks to issue payment cards and merchants to accept those cards. It is a small fee paid by the acquirer to the issuer and serves to compensate the issuer for a portion of the risks and costs it incurs to maintain cardholder accounts. These costs include finance costs for the interest-free period between the time a cardholder makes a purchase and pays his or her bill, credit losses, fraud protection, and processing costs.

By shifting some of the cost of the payment system from issuers and their cardholders to acquirers and their merchants, a system operator like MasterCard can encourage greater use of its cards. Often referred to as "balancing the system," this makes the system more efficient and valuable to cardholders and to merchants.

When a purchase is made with a payment card, the acquirer pays the issuer an interchange fee to help offset a portion of these costs. The acquirer eventually collects this fee from the merchant as a component of the merchant discount fee.

Merchant Discount Fee

The merchant discount fee is generally a small percentage of the price of the goods or services the merchant pays its acquirer when a payment card is used. The merchant discount fee is negotiated between the merchant and its acquirer. MasterCard is not a party to this contract nor does it have a role in the negotiation between the merchant and its acquirer.

Interchange Rates

MasterCard interchange rates are established by MasterCard and are generally paid by acquirers to issuers on purchase transactions conducted with MasterCard cards. MasterCard has no involvement in acquirer and merchant pricing policies or agreements.

Interchange rates are a necessary and efficient method by which MasterCard maintains a strong and vibrant payments network. Setting interchange rates is a challenging proposition that involves an extremely delicate balance. If interchange rates are set too high, such that they lead to disproportionately high MDRs, merchants' desire and demand for MasterCard acceptance will drop. If interchange rates are set too low, issuers' willingness to issue and promote MasterCard cards will drop, as will consumer demand for such cards. In response to these competitive forces, MasterCard strives to maximize the value of the MasterCard system (including the dollars spent on MasterCard cards, the number and types of cards in circulation, and the number and types of merchants accepting MasterCard cards) by setting default interchange rates at levels that balance the benefits and costs to both cardholders and merchants.

MasterCard has published interchange rates that apply to U.S. merchants' transactions, which include U.S. interchange rates (that is, the interchange rates that apply to transactions conducted on a U.S.-issued card at a U.S. merchant) and Interregional interchange rates (the interchange rates that apply to transactions conducted on a non–U.S.-issued card at a U.S. merchant).

To help you determine which of the many interchange rates may apply to your transaction, see the *MasterCard Worldwide U.S. and Interregional Interchange Rates*.

The *MasterCard Worldwide U.S. and Interregional Interchange Rates* document contains the following information:

- Merchant categories, key criteria associated with each interchange rate, and a Glossary of Terms

- Interchange rate tables organized by product type

- Each interchange rate has a series of requirements, all of which must be satisfied for a transaction to qualify for that rate

- Requirements include factors such as merchant category; the time between authorization and clearing; the presence or absence of magnetic stripe data; the submission of enhanced transaction data; and a merchant's MasterCard sales and transaction volume. MasterCard systems ensure that all requirements are met when a transaction is submitted for a particular interchange rate.

Merchants and acquirers should strive to meet all of the criteria necessary to qualify transactions for the rate that are most advantageous to them.

Merchant Classifications

The following list provides merchant classifications. Merchants should identify the merchant classification that most closely relates to their line or lines of business to determine which interchange rates may apply to their transactions:

- Airline and Passenger Railway

- Cruise Line

- Gas Stations and Convenience Stores

- Government

- Lodging and Vehicle Rental

- Restaurant

- Retail/Services

- Supermarket/Warehouse

- Transportation and Tolls

- Travel Agencies

- Utilities

To help you determine which of the many interchange rates may apply to your transaction, see the *MasterCard Worldwide U.S. and Interregional Interchange Rates*.

Card Acceptor Business Codes

Formerly referred to as merchant category codes, card acceptor business codes (MCCs) are four-digit numeric codes that represent the merchant's primary business and facilitate risk management.

Updating Rates

MasterCard interchange rates are typically updated semiannually. MasterCard publishes interchange rates and related criteria on the merchant Web site (www.mastercardmerchant.com) generally concurrent with each rate update. While MasterCard will endeavor to keep the rates and related criteria on the Web site up to date, it is possible that this Web site will not be absolutely current in all regards. In the event of any discrepancy between the rates and criteria found in this document and those rates and criteria MasterCard deems to be the official rates and criteria, the official rates and criteria will apply.

MasterCard is confident that the *MasterCard Worldwide U.S. and Interregional Interchange Rates* document gives you the information needed to understand the interchange rates and structure and determine which rates may apply to your transactions. However, MasterCard also recognizes that this information is being made available to a very diverse audience, with diverse needs and expectations. MasterCard encourages merchants to speak with their acquirer or member service provider (MSP), if they have questions regarding any aspect of MasterCard interchange rates, acceptance of MasterCard cards, or their card acceptance agreements.

Chapter 7   Chargeback Support

This chapter provides a high-level overview about chargeback requirements and best practices.

Overview

This chapter provides a high-level overview about chargeback requirements and best practices.

For detailed information about chargebacks, see the *Chargeback Guide.* For information about chargeback rules, see the *MasterCard Rules* and *Maestro Global Rules.*

What is a Chargeback

A chargeback is a procedure in which an issuer charges all or part of the amount of an interchange transaction back to the acquirer in accordance with MasterCard regulations.

After the initial presentment of a cardholder transaction from the acquirer to the issuer, the issuer may determine that, for a given reason, the transaction may not be valid. The issuer may return the transaction to the acquirer as a chargeback. The issuer can submit a chargeback if the issuer or the cardholder disputes the first presentment. The chargeback must be processed within the designated time frames after receiving the first presentment. (These time frames vary according to the chargeback reason.) This returns the transaction to the acquirer for possible remedy.

Why Do Chargebacks Occur

Chargebacks fall into five categories:
- Authorization
- Fraud
- Cardholder disputes
- Retrieval request and documentation required
- Errors in processing or procedure

Chargebacks usually happen when there is a customer dispute or an error on the dollar value of the transaction—and financial liability—is typically reversed back to the merchant.

What is the Chargeback Process

After the first presentment of a transaction from the acquirer to the issuer, the issuer may determine that the transaction may be invalid. The issuer may then return the transaction to the acquirer as a chargeback for possible remedy. The chargeback process or dispute resolution process is used by members to determine the responsible party in a chargeback related dispute.

Following the first presentment of a transaction, the chargeback life cycle includes:
- First chargeback (submitted by the issuer)

- If necessary, a second presentment (submitted by the acquirer)
- If necessary, arbitration chargeback (submitted by the issuer)

Applicable time frames associated with the generation of a first chargeback depends on the message reason code. If the members do not resolve the case within three cycles, they must send the case to arbitration. Additionally, if an issuer needs a copy of the transaction information document (TID), the retrieval process has two steps—Retrieval Request and Retrieval Fulfillment. The retrieval process may also include Image Review.

Retrieval Requests and Retrieval Fulfillment

An issuer can request the transaction slip from the acquirer if there is any question about the transaction that the original document or facsimile may resolve. To complete this cycle, the acquirer either fulfills the issuer's request or sends a message documenting the inability to honor the request. MasterCard encourages the use of the MasterCom® electronic imaging system to deliver transaction slips and other information concerning the request.

Message Reason Codes

This following information lists chargeback message reason codes in number order by category.

Authorization-related Chargebacks

The following message reason codes are authorization-related chargebacks:
- 4807—Warning Bulletin File
- 4808—Requested/Required Authorization Not Obtained
- 4812—Account Number Not On File

Fraud-related Chargebacks

The following message reason codes are fraud-related:
- 4837—No Cardholder Authorization
- 4840—Fraudulent Processing of Transactions
- 4847—Requested/Required Authorization Not Obtained and Fraudulent Transaction
- 4849—Questionable Merchant Activity
- 4862—Counterfeit Transaction Magnetic Stripe POS Fraud
- 4863—Cardholder Does Not Recognize—Potential Fraud (Arbitration chargeback message reasons RS2 and RS3)
- 4870—Chip Liability Shift
- 4871—Chip/PIN Liability Shift

Cardholder Dispute Chargebacks

The following message reason codes apply to cardholder disputes:

- 4841—Cancelled Recurring Transaction
- 4853—Cardholder Dispute—Defective Merchandise/Not as Described
- 4854—Cardholder Dispute—Not Elsewhere Classified (U.S. region only)
- 4855—Nonreceipt of Merchandise
- 4857—Card-Activated Telephone Transaction
- 4859—Services Not Rendered

Retrieval Request and Documentation Required

The following message reason codes apply to chargebacks for retrieval request and documentation-related chargebacks:

- 4801—Requested Transaction Data Not Received
- 4802—Requested/Required Information Illegible or Missing
- 4863—Cardholder Does Not Recognize—Potential Fraud (First chargeback only)

Errors in Processing or Procedure

The following message reason codes generally apply to errors in processing or procedure:

- 4831—Transaction Amount Differs
- 4834—Duplicate Processing
- 4835—Card Not Valid or Expired
- 4842—Late Presentment
- 4846—Correct Transaction Currency Code Not Provided
- 4850—Credit Posted as Purchase
- 4860—Credit Not Processed

Maestro Message Reason Codes

This following information lists Maestro chargeback message reason codes.

Chargeback Reason Codes

The following chargeback reason codes are applicable for all regions except the Europe region. For information about Europe region chargeback reason codes, refer to Europe Region Message Reason Codes for Interregional Transactions. All chargebacks for POS transactions must be processed using the applicable chargeback reason codes documented below.

Chargeback Reason	Reason Code	PIN-Based	Signature
Transitional Chip Liability Shift	70	X	X
Disputed Amount (POS/electronic commerce Transactions only)	71	X	X
Credit Posted as Debit (POS/electronic commerce Transactions only)	72	X	X
Duplicate Transaction (For POS/electronic Transactions only)	73	X	X
Missing or Illegible Signature (POS Transactions only)	74	N/A	X
Credit Not Received (POS/electronic commerce Transactions only)	75	X	X
Documentation Not Received on Retrieval request (POS Transactions only)[1]	76	X	X
Cardholder Denies Transaction Finalized (POS/electronic commerce Transactions only)	77	X	X
Documentation Not Legible on Retrieval Request (POS Transactions only)[1]	78	X	X
Goods or Services Not Delivered (electronic commerce Transactions only)	79	X	N/A
Late Presentment	80	X	N/A

---

1.   This Transaction is not currently supported in the Single Message System.

Europe Region Message Reason Codes for Interregional Transactions

The following message reason codes are applicable to interregional POS, e-commerce, PIN-based in-branch, and Maestro *PayPass* transactions, unless otherwise indicated under the message reason code.

Chargeback Reason	Europe Members use Reason Code	Members outside Europe use Reason Code	PIN-based?	Signature?
Cardholder Denies Transaction Finalized **(POS and e-commerce transactions only)**	4515	77	Yes	Yes
Documentation Not Received on Retrieval Request **(POS transactions only)**[2]	4801	76	Yes	Yes
Documentation Not Legible on Retrieval Request **(POS transactions only)**[2]	4802	78	Yes	Yes
Disputed Amount **(POS and e-commerce transactions only)**	4831	71	Yes	Yes
Duplicate Transaction	4834	73	Yes	Yes
Missing or Illegible Signature or No Cardholder Authorization **(POS transactions only)**	4837	74	N/A	Yes
Credit Posted as Debit **(POS and e-commerce transactions only)**	4850	72	Yes	Yes
Goods or Services Not Delivered **(e-commerce only)**	4855	79	Yes	N/A
Credit Not Received **(POS and e-commerce transactions only)**	4860	75	Yes	Yes
Chip Liability Shift **(POS Transactions Only)**	4870			
Chip Transaction—Late Presentment **(POS Transactions Only)**	4880	80	Yes	No

---

2. This chargeback is not currently supported in the Single Message System.

Chapter 8   Controlling Fraud

This chapter explains types of card fraud and how merchants can prevent fraud. A merchant fraud checklist is also provided.

Types of Card Fraud

The following is a list of the three main types of card fraud:

- **Altered/Counterfeit Cards**—On an altered card, the name, expiration date, account number, and/or the magnetic stripe have been changed in some way. Counterfeit cards are "fake" manufactured cards that bear a valid account number. A valid card number may appear on the front of the card, in the magnetic stripe on the back of the card, or in both places.

- **Lost/Stolen Card**—A card is stolen from the cardholder and used fraudulently to purchase goods or services from a legitimate merchant.

- **Card Not Present Fraud**—Someone other than the authorized cardholder obtains a MasterCard account number (often with the expiration date of the account and CVC 2 from the back of the card) and uses it to purchase goods or services on the Internet, by mail, or by phone.

Fraud Prevention

MasterCard has established security procedures that can help you protect your business from loss.

When You Suspect Fraud

If your employees are suspicious about a card or a cardholder at any time during a transaction, tell them to call the Authorization Center and request a Code 10 authorization.

A Code 10 authorization request alerts the issuer to suspicious activity—without alerting the customer. During a Code 10 call, your acquirer may ask for transaction details. Your staff will be transferred to the issuer's special operator who will provide instructions on any necessary action.

In-store, Card Present Fraud

If your employees suspect fraud, train them to remain calm and call the Voice Authorization Center immediately. When the operator picks up, train your staff to say, "I have a code 10 Authorization Request," and then follow these steps:

- Stay calm to avoid alarming the person who presented the card.

- Keep the card in question in your hand.

- Answer the operator's questions in a normal tone with a simple "yes" or "no."

- Follow the operator's instructions.

- For your staff's safety, do not, under any circumstances, confront or try to apprehend the customer.

If it becomes necessary to notify the police, the operator will do so while your employee waits on the line.

Reporting Fraud

Sometimes fraud happens even with strong preventive measures in place. Keep contact information for reporting fraud easily accessible, and make sure your employees know how to use it.

If a fraudulent transaction occurs, contact the following for assistance:
- Your acquirer or member service provider (MSP)
- Your legal counsel
- Your local police department or U.S. Secret Service office

Unsigned Credit Cards

MasterCard rules and security procedures require that credit cards must be signed by the cardholder to be accepted for payment. The signature on the back of the card is one of a multi-layered set of security protections in place for cardholders and merchants. The presentation of a signed card allows the merchant to verify the cardholder's identification by comparing the signature on the card to that on the sales receipt.

If an unsigned card is presented, the merchant must:
- Obtain usual authorization for the transaction
- Ask the customer to provide confirming identification
- Require the cardholder to sign the card. The merchant must not complete the transaction if the cardholder refuses to sign the back of their card.

If the card says "Ask for Photo ID" in the signature space, the transaction cannot be processed, unless the cardholder's signature appears in the signature space. Cards are not valid unless signed.

Online and Telephone Transactions

MasterCard card verification and security programs enable cardholders to feel more confident about conducting online, mail order, and telephone transactions. The following information will help you keep these kinds of transactions secure.

Avoid Fraud on Card-Not-Present Transactions

Fraud is a particular concern for mail order, telephone order, and Internet businesses because transactions are card-not-present. Businesses can minimize the occurrence of fraudulent transactions through a number of safeguards:
- Before shipping merchandise, call the phone number the customer provided and verify the transaction information. Often, fraudsters are unable to verify the information they originally provided because they order at random and do not keep a record of what they requested.
- Be sensitive to priority shipments for fraud-prone merchandise, which may indicate a fraudulent transaction.

- Be wary of orders from past customers that differ from their usual purchasing patterns.

Participate in Cardholder Verification Programs

To address the unique concerns of direct marketers, MasterCard recommends using the Address Verification Service (AVS), when available and Card Validation Code 2 (CVC 2) verification, when available. These highly effective cardholder verification programs can make transactions safer and more profitable.

For more information about these cardholder verification programs, see Cardholder Verification Programs.

Protect Online Transactions with MasterCard *SecureCode*

MasterCard® *SecureCode*™ makes online shopping more secure for merchants and their customers by providing cardholders with a unique personal code for their transactions. In addition to helping prevent chargebacks and fraud, *SecureCode* can give customers greater peace of mind and allow electronic merchants to ship orders with confidence. It's a simple, cost-effective way to encourage e-commerce while reducing risk.

For information about *SecureCode*, see MasterCard SecureCode. For more information about becoming a *SecureCode* merchant, go to www.securecodemerchant.com.

Protect Data by Achieving and Maintaining PCI Compliance

You can help protect your business and your customers against hackers and other security challenges by becoming PCI compliant. The MasterCard Site Data Protection program provides the requirements, guidelines, and tools that improve your security posture by identifying vulnerabilities in your systems and helping you understand how to greatly reduce the risk of having your customers' data compromised.

For more information about the MasterCard Site Data Protection Program, go to www.mastercard.com/us/sdp/index.html.

Merchant Fraud Checklist

Each time a customer presents a MasterCard card, your staff should go through the following checklist:

1. **Check the embossed numbers on the front of the card**

   All MasterCard account numbers start with the number 5. If an account number is embossed, the embossing should be clear and uniform in size and spacing, and extend into the hologram (if a hologram is on the card face). The last four digits of the account number on the front of the card should match the four digits printed on the signature panel on the back of the card. These numbers should not be chipped away and no "halos" of previous numbers should appear under the embossed account number.

2. **Examine the hologram**

   A MasterCard hologram is usually on the front of a MasterCard card either above or below the MasterCard Brand Mark. On some new card designs, the hologram may be on the back of the card or integrated into the magnetic stripe on the back of the card. The three-dimensional hologram with interlocking globes should reflect light and appear to move when the front of the card is rotated.

3. **Compare signatures**

   The back of the card must be signed, and the signature should reasonably compare to the cardholder signature on the sales receipt. Check to be sure that it has not been taped over, mutilated, erased, or altered in any suspicious manner. The word "Void" on the signature panel indicates that the signature panel has been tampered with.

4. **Look at the magnetic stripe**

   The magnetic stripe on the back of the card should appear smooth and straight, with no signs of tampering.

5. **Become familiar with new card designs**

   Effective in 2009, any MasterCard card may be issued unembossed. This is a card design option. These cards may look different—they have no raised (embossed) numbers—so you cannot make a manual imprint, but the brand behind them is the same. Your business must have an electronic terminal to accept these cards.

6. **Examine the expiration date**

   The card should not be accepted after the last day of the "valid through" date embossed on the card. Merchant clerks must validate the card expiration date.

7. **Is the customer using the card the actual cardholder?**

   A MasterCard card is non-transferable. Check to see that the signature on the sales receipt matches the signature on the back of the card. Be observant of the customer's behavior—does it seem normal or does the person appear uneasy?

If any suspicious behaviors occur, you can ask for help. If an employee is at all suspicious about a card, call your Voice Authorization Center and request a Code 10 Operator. The Authorization Center will help you decide whether to complete the transaction.

Appendix A   Glossary

This appendix provides a glossary of terms, concepts, acronyms, and abbreviations used in MasterCard publications.

A

account data compromise event (ADCE)—An event in which account data may have been compromised that could lead to unauthorized use of the cardholder's account. An account data compromise event does not mean that account data was wrongfully disclosed or used, but that account data may have been wrongfully disclosed or used.

acquirer—A member that maintains the merchant relationship and acquires the data relating to a transaction from the merchant or card acceptor.

Address Verification Service (AVS)—A MasterCard service to help combat fraud for non–face-to-face transactions by use of cardholder address information in the authorization request.

affiliate member—A type of MasterCard member that participates indirectly through an association member or a principal member in the activities of this Corporation (for example, by issuing MasterCard® cards or by accepting transaction records from merchants).

authentication—In security, ensuring that the message is genuine, that it has arrived exactly as it was sent, and that it comes from the stated source.

authorization—Approval of a transaction by or on behalf of an issuer according to defined operations regulations. The merchant receives, via telephone or authorization terminal, this approval to process the transaction.

authorization code—A six-digit alphanumeric code assigned by the issuer to identify the approval for a specific authorization request. Also referred to as "issuer's response code," "authorization approval code," or "authorization response code."

authorization message—Within a payment system, any message between a card acceptor and an issuer serving to establish whether the issuer approves for a transaction to proceed.

authorization response—Answer to an authorization request, typically a code, that advises the acquirer or merchant how to proceed with the transaction.

Automated Clearing House System (ACH)—One of the group of processing institutions that network together to exchange (clear and settle) electronic transactions.

automated fuel dispenser (AFD)—A terminal device used to accept payment for fuel at a petroleum service station.

B

bank identification number (BIN)—A unique six-digit number assigned by MasterCard International to identify acquiring members. The BIN is contained in DE 31 (Acquirer Reference Data), positions two through seven.

bankcard—A payment card issued by a bank or other financial institution, such as a MasterCard® or Maestro® card.

batch processing—A type of data processing operation and data communications transmission where related transactions are grouped together and transmitted for processing, usually by the same computer and under the same application; generally regarded as non–real-time data traffic comprising large files; type of data traffic where response time is not critical.

brand mark or mark—The proprietary combination of names, symbols, and colors that visually conveys a brand's identity and personality.

C

call referral—A generic term for the "refer to card issuer" authorization response. A call referral indicates that the acquirer or merchant must contact the issuer for further instructions. The issuer uses the call referral as a fraud prevention tool when it suspects or is attempting to prevent fraud at the point of interaction.

card acceptor—A merchant or an ATM that accepts a card and presents transaction data to an acquirer.

card acceptor business code (MCC)—A numerical representation of the type of business in which the card acceptor (merchant) engages. Formerly merchant category code (MCC).

card account—A credit line for deposit facility accessed by a card issued to a cardholder that enables the cardholder to purchase goods and services or obtain cash.

card payment system—A payment system supporting payments made by financial transaction cards.

card validation code (CVC)—A card security feature. CVC 1 is a three-digit value encoded on Tracks 1 and 2 in three contiguous positions in the discretionary data field of a magnetic stripe on a MasterCard card or Maestro card. CVC 2 is indent-printed into the tamper-evident signature panel on a MasterCard card. Chip CVC is a three-digit value encoded in the Track 2 Equivalent Data field in three contiguous positions within the discretionary data field of the chip on a MasterCard card or Maestro card. The CVC is intended to inhibit the alteration or misuse of card data and enhance the authentication of the card.

Although a CVC code may appear on Maestro cards, it is not mandatory.

chargeback process—A dispute resolution process that members use to determine the responsible party in a chargeback related dispute. This process has three cycles in which the members can resolve the dispute themselves. If the members do not resolve the case within three cycles, they must send the case to arbitration.

These three cycles are:

- First chargeback (submitted by the issuer)
- Second presentment (submitted by the acquirer)
- Arbitration chargeback (submitted by the issuer)

clearing—The process of exchanging financial transaction details between an acquirer and an issuer to facilitate posting of a cardholder's account and reconciliation of a customer's settlement position.

co-branded card—A card issued by a member in association with a commercial company, typically bearing the brand of both

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

credit card—A plastic card bearing an account number assigned to a cardholder with a credit limit that can be used to purchase goods and services and to obtain cash disbursements on credit, for which a cardholder is subsequently billed by an issuer for repayment of the credit extended at once or on an installment basis.

credit loss—The amount lost (charged off) as a result of failure of the cardholder to pay the amount owed on the account

cross-border transaction—Any transaction on a MasterCard credit or debit card or Maestro card processed through the Global Clearing Management System (GCMS) or the MasterCard® Debit Switch (MDS) in which the country code of the merchant differs from the country code of the cardholder.

D

debit card—A plastic card used to initiate a debit transaction. In general, these transactions are used primarily to purchase goods and services and to obtain cash, for which the cardholder's asset account is debited by the issuer.

debit transaction—A transaction initiated when a card is presented as payment for goods and services or at an ATM for cash withdrawals. The transaction amount is automatically deducted from the cardholder's demand deposit or other bank account.

E

e-commerce transactions—The non–face-to-face payment for goods or services by use of electronic media over a public network (such as the Internet) or private network (such as an extranet).

electronic commerce—The exchange of goods and services for payment between the cardholder and merchant. The transaction is performed (completely or partially) via electronic communication.

electronic draft capture (EDC)—(Generic) A system in which the transaction data is electronically captured at the merchant location for authorization and clearing processing.

electronic funds transfer (EFT)—A paperless transfer of funds initiated from a terminal, computer, telephone instrument, or magnetic tape.

Electronic Funds Transfer System (EFTS)—An electronically based system designed to eliminate the paper instruments that are normally associated with fund movement. For example, a cash withdrawal from an ATM that eliminates the check.

electronic point of sale—A point-of-sale merchant equipped with electronic equipment for pricing and recording transactions, but not necessarily incorporating functions for electronic funds transfer (EFT).

Emergency Card Replacement Service (ECR Service)—The MasterCard worldwide service designed to provide temporary cards to all MasterCard cardholders that do not have their cards in their possession. This card is issued to a cardholder that needs a temporary replacement card sooner than the typical five to 10 days that it takes to get a permanent card.

F

face-to-face transaction—A transaction where the card, the cardholder, and the merchant are all present at the time of the transaction.

financial institution—Any commercial bank, federal or state savings and loan association, federal or state savings bank, or credit union.

First chargeback—A procedure in which an issuer charges all or part of the amount of an interchange transaction back to the acquirer in accordance with MasterCard regulations.

fraudulent merchant—A retailer, or any other person, firm, or corporation that agrees to accept credit cards, debit cards, or both; and engages in an unauthorized transaction occurring on any of the cards offered by MasterCard.

G

guaranteed reservation—Use of a MasterCard account number to reserve accommodations at lodging merchants. For the cardholder, such reservations include a late arrival provision, penalties if cancellation rules are not met, and a provision for unavailable rooms upon arrival.

guest folio—A lodging merchant's guest record that contains the cardholder's transaction information, including check-in and departure dates, rate, anticipated length of stay at check-in time, applicable charges, and taxes. The check-in date and the dated amount and authorization approval code of each authorization must be included on the folio if not on the sales draft.

I

Independent Sales Organization (ISO)—An MSP that provides Program Services other than transaction and cardholder processing to a member in support of the member's program. Such program services include, but are not limited to, merchant solicitation, cardholder solicitation, customer service, and ATM deployment.

in-flight commerce—Transactions such as shopping or gaming activity that a cardholder initiates during a flight. In MasterCard applications, these transaction types also are referred to as Cardholder-Activated Terminal (CAT) Level 4.

interchange—The exchange of transaction data between acquirers and issuers in accordance with MasterCard rules.

interchange fee—A fee applied to an interchange transaction, applicable to the two members participating in the transaction as issuer and acquirer.

interchange program—A program that reimburses issuers for specific costs related to an incoming interchange transaction. These costs include processing costs, financial carrying costs, and risk costs. Interchange fees are payable to the issuer by the acquirer.

issuer—A licensed MasterCard member that issues cards or access devices to accountholders.

M

magnetic stripe—The magnetically encoded stripe on the bankcard plastic that contains information pertinent to the cardholder account. The physical and magnetic characteristics of the magnetic stripe are specified in ISO Standards 7810, 7811, and 7813.

magnetic stripe reader—A device that reads information recorded on the magnetic stripe of a card.

mail order/telephone order (MO/TO)—A transaction initiated by mail or telephone to be debited or credited to a bankcard account.

MasterCard account number—A 16-digit number, beginning with the number 5, assigned by an issuer to uniquely identify a MasterCard account that conforms to the MasterCard defined structure and check-digit specifications.

MasterCard Brand Mark—The interlocking circles used in conjunction with the MasterCard logotype, positioned and proportioned exactly as shown in authorized reproduction artwork.

MasterCard Payment Gateway (MPG)—A gateway hosted by MasterCard and used for routing and settling commercial e-payments between buyers and suppliers.

MasterCard® SecureCode™—MasterCard *SecureCode* is a program supporting cardholder authentication and guaranteed payments over the Internet for MasterCard and Maestro transactions.

Member Service Provider (MSP)—A non-member that is registered by MasterCard International Incorporated as an MSP to provide Program Services to a member, or any member that is registered by MasterCard International Incorporated as an MSP to provide Third Party Processor (TPP) Program Services to another member. MSPs are classified in two categories: ISO and TPP.

merchant—A merchant is a commercial entity or person that pursuant to a merchant agreement is authorized to accept cards and access devices when properly presented.

merchant agreement—A written agreement between a merchant and an acquirer containing their respective rights and performance obligations with respect to card acceptance.

merchant authorization—The means receiving sales validation for the merchant, by telephone or authorization terminal to provide chargeback protection to the merchant.

merchant bank—A bank that has entered into an agreement with a merchant to accept deposits generated by bankcard transactions; also called the acquirer or acquiring bank.

merchant ID number—A unique number assigned by the acquirer to identify the merchant.

N

non–face-to-face transaction—A transaction where the card, the cardholder, and/or the merchant is not present at the time of the transaction. Mail order, telephone order, cardholder-activated terminal (CAT), electronic commerce, and transponder are examples of non–face-to-face transactions. See also card not present.

O

offline—An operating mode in which a card acceptance device is not connected to a central computer source. Responses are governed by the parameters or guidelines set within the terminal or supporting device as defined by the issuer or MasterCard. The accessibility of information is not in a live environment, meaning that current active files are not being viewed during the time the transaction is conducted.

online—An operating mode in which a card acceptance device is connected to a central computer system and has access to the database for authorization, inquiry, and file changes. Live files are accessed for each transaction. For authorization, an operating mode in which members are directly connected to the MasterCard Worldwide Network via a MIP or their host computer. Live files are accessed for each transaction.

P

personal identification number (PIN)—A four- to 12-character alphanumeric code that enables an issuer to authenticate the cardholder to approve an ATM or terminal transaction occurring at a point-of-interaction (POI) device.

point of interaction (POI)—The location where a transaction occurs (formerly point of sale or point of service).

point-of-sale system—An electronic system that accepts financial data at or near a retail selling location and transmits that data to a computer or authorization network for reporting activity, authorization, and transaction logging.

Portable Document Format (PDF)—A file format that allows files or documents saved using Adobe Acrobat software to be displayed and printed in exactly the same format on another platform.

prepaid card—A card that stores value and is used instead of cash to pay for a single service, such as pay telephones or public transportation. It cannot be reloaded and is a throwaway or collector card.

processing fee—Compensation paid by issuers or acquirers to a financial network organization for processing interchange transactions according to the business agreements established by that financial network. Fees are determined by each transaction type for issuers and acquirers participating within each individual financial network.

processor—An organization that is affiliated with MasterCard International Incorporated. The processor provides authorization and/or clearing services on behalf of a member. The processor also provides settlement support services on behalf of the member. However, in accordance with MasterCard rules, processors are prohibited from taking possession of or owning settlement funds.

promotion code—A code assigned by the issuer to identify transactions that apply to a promotional program run by the issuer to encourage card use.

proprietary card—A type of card that financial institutions or other organizations issue using the logo of the issuer instead of a national service mark or logo (such as MasterCard). A proprietary card allows the cardholder to access a credit or deposit account using ATM or POI terminals.

purchase—A financial transaction, if approved, in which funds are debited from an issuer and credited to an acquirer in payment for goods or services.

Q

Quick Payment Service (QPS)—The MasterCard program designed to facilitate new penetration of card acceptance by targeting cash and convenience-oriented merchant segments, for example, fast food chains, movie theaters, and parking lots.

R

recurring payments—Payments by an issuer to an acquirer on behalf of a cardholder who authorizes a merchant to bill the cardholder's account on a recurring basis (such as monthly or quarterly). The amount of each payment may be the same or may fluctuate.

refund—Opposite of a purchase transaction, namely, the cardholder returns goods to the merchant and is credited for their value. Positive interchange and merchant service charge are reversed

retail banking—The part of a bank's operations providing services at its branches for small or individual account holders.

retail sale transaction—Purchase of goods, services, or both, generally at a merchant establishment.

S

self-service terminal—A customer activated terminal, especially one including the functions of both delivering and paying for goods (for example, in an automatic fuel vending system).

Standards—As used by MasterCard, "Standards" means the bylaws, rules and policies, and the operating regulations and procedures of MasterCard International Incorporated, as may be amended from time to time.

store card—A financial transaction card associated with a particular retailer or group of retail stores that can be used only for purchases from that retailer or group of stores.