Card Acceptance Guide

Your Guide to Debit and Credit Acceptance and Processing

Moneris SOLUTIONS

Important Information

Your merchant account representative _____

Merchant Help Desk _____

Telephone authorization number _____

Merchant ID number _____

Terminal ID number _____

To verify issuing bank, call:

MasterCard®	1-800-622-7747
Visa®	1-800-VISA-750 1-800-847-2750
Discover®	1-800-347-1111
American Express®	1-800-528-2121

Other _____

_____

1350 Independence St. | Denver, CO 80215

Merchant Guide to Card Acceptance

What's in this guide?

This quick-reference booklet will help you take full advantage of the benefits of accepting credit and debit cards. It explains acceptance and processing procedures, and offers tips to help you optimize your profits from these sales. We have provided you with this booklet because, as your merchant acquirer, we have a vested interest in the success and growth of your business. Please follow these guidelines.

This guide is part of your Merchant Agreement with us. In order to remain in compliance with that agreement and retain your card acceptance privileges, you must follow the requirements and procedures outlined in this guide.

How to use this guide

We've provided a Table of Contents on p. 3 and a Definitions section on p. 22, where you'll find definitions for the terms that appear in this guide.

We're here to help

We work hard to make sure your card acceptance program works efficiently and is flexible enough to grow and change with your business. If you have questions or comments we haven't covered in this guide, please contact your merchant representative.

Card acceptance supplies

Your Merchant Welcome Kit should contain everything you need to begin card acceptance. If you need to order additional supplies, you should contact customer service.

Beware of draft laundering

Depositing sales slips that are not yours is called "draft laundering" or "factoring." This practice is in violation of your merchant agreement and could result in chargebacks, termination of your card acceptance privileges and criminal prosecution. If anyone asks you to deposit payment card sales slips on their behalf, report the incident immediately to us and to the U.S. Secret Service.

Table of Contents

Card Basics 4
- How cards work 4
- Issuance 4
- Acceptance 4
- Settlement 4

Accepting Cards 5
- Which cards can you accept? 5
- General acceptance guidelines 6

Card Identification Features 7
- How to determine if a card is valid or fraudulent 7
- Visa card features 8
- MasterCard card features 9
- Discover Card features 10
- American Express card features 11
- What to do with an unsigned card 12
- Warning signs of fraud 12
- Code 10 procedures 13

Processing Transactions 14
- Electronic processing 14
- Processing key-entered transactions 15
- Telephone authorization and manual processing 16
- Processing returns 17
- Processing mail, telephone and Internet orders 17
- Processing preauthorized orders/recurring payments 18
- Touch-tone processing 18

After the Sale 18
- Closing out your electronic terminal 18
- Adjustments to your account 19
- Chargebacks and retrievals 19
- Tips to reduce chargebacks 21
- Draft retrieval request 21

Definitions 22

Card Basics

How cards work

Credit and debit cards issued by financial institutions are a convenient alternative to cash and checks. MasterCard and Visa, along with American Express and Discover® Cards, are now accepted by millions of merchants worldwide. Payment cards are generally issued by a bank, credit union or other financial institution. American Express and Discover, while not banks, are also called card issuers.

Payment cards include both credit cards and debit cards. A credit card accesses a credit account, while a debit card accesses funds in a deposit account (checking account).

Processing credit and debit cards involves three basic elements: issuance, acceptance and settlement.

Issuance

To issue MasterCard, Visa, American Express or Discover Cards, a card issuer must first enter a membership agreement with one or more of the card associations (MasterCard or Visa). Many issuers offer both MasterCard and Visa cards. American Express and Discover issue cards either directly to consumers or through financial institutions.

To obtain a credit or debit card, your customer opens a deposit or credit account with a card issuer. Your customer may have cards from several different issuers.

Acceptance

Your Merchant Agreement with us specifies which cards you can accept: Visa, MasterCard, American Express, Discover or other. Details of the acceptance process begin on page 5.

Settlement

You receive payment for transactions you accept through a process called settlement. When your customer uses a card at your business, the card issuer pays you on behalf of your customer via a credit posted electronically to your merchant account. The card issuer then bills your customer.

In most transactions, that's all there is to it. Occasionally, processing errors or customer questions about a transaction may occur. Please refer to pp. 18–21 for more on how such errors and questions are handled.

Accepting Cards

Which cards can you accept?

Your Merchant Agreement specifies which card types you should honor. You can accept them with confidence when you follow the guidelines in this booklet. In addition to Visa, MasterCard, American Express and Discover Credit Cards, your customers may present any of the following:

MasterCard, Visa and Discover debit cards

You are authorized to accept all debit cards. Debit cards resemble Visa, MasterCard and Discover Credit Cards (see pp. 8–10). Newer Visa debit cards will have the word "Debit" printed on the front above the hologram. Most MasterCard debit cards will have a unique debit hologram, while some will have the word "Debit" printed on the front. On Discover Debit Cards, the name "DEBIT" must appear anywhere within the gray shaded area on the front of the card.

Debit cards can be authorized using offline or online systems. Online cards are authorized through the debit card networks for funds availability, and require entry of a Personal Identification Number (PIN). Authorizing debit cards in the offline mode requires a customer's signature on the sales slip instead of a PIN entry.

International cards

Credit and debit cards are issued by financial institutions throughout the world. You can accept any valid card, regardless of where it was issued. If you are a U.S. merchant, all payment card transactions you accept are processed in U.S. funds. Conversion differences are applied to cardholder accounts without affecting cash value to you.

Other types of cards

There are a wide variety of other card types in today's marketplace. Stored value cards, including payroll cards, gift cards and travel money cards, will all bear the name and brand mark of one of the card associations. These cards should display the same basic features you look for on credit and debit cards (see pp. 8–11).

General acceptance guidelines

- Do not charge fees or impose restrictions. The card associations and/or Discover prohibit you from adding a surcharge, assigning a minimum or maximum purchase amount or imposing other restrictions on card transactions.
- Do not process split sales. Attempting to avoid authorization (required on all transactions) by processing partial transaction amounts on separate sales slips is prohibited by the card associations and/or Discover, and will result in chargebacks.

Protect your customers

Never record a customer's address, phone number, photo ID number or other personal information on a payment card sales slip. You can record such information elsewhere if your telephone authorization center requests it (see p. 16) or if you need it to deliver merchandise. Here are a few other things you should do to protect your customers' safety and privacy:

- Store card sales slips in a secure area, accessible only to select personnel.
- Destroy any documents showing card account numbers before discarding them.
- Provide space on the inside of your mail-order forms for card account numbers, expiration dates, phone numbers and other sensitive information.

Data security

With the explosive growth of identity theft, data security has become more than just important — it's mandatory. In an effort to slow the continued growth of identity theft, Visa, MasterCard, American Express and Discover have collaborated in creating a worldwide standard for consumer data protection. This common approach combines Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection (SDP) Program, Discover Information and Security Compliance (DISC) and American Express' Data Security Operating Policy (DSOP).

The result is a global data security standard called the Payment Card Industry (PCI) Data Security Standard. This unilateral approach provides merchants with a single validation process to assess their security across all card platforms. As a merchant accepting credit and debit cards, you are required by the card associations and/or Discover, to adhere to the PCI Standard, outlined on the following page.

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Card Identification and Features

How to determine if a card is valid or fraudulent

The first step in accepting a card is making sure the card is valid. Examine every card presented to you to be sure it has the features outlined below and on the following pages. If features are missing or altered, call your telephone authorization number for a Code 10 (see p. 13). (Note: Some features pictured in this guide are optional, and do not appear on all valid cards.)

The following are features you should check for on every card:

- Overall appearance: Check for discoloration or uneven card surfaces.
- Embossing: Card account number, valid dates, cardholder name and security character should appear consistent in size and spacing and should not look "ghosted" (new characters re-embossed over originals).
- Valid dates or expiration date: Make sure the card is not expired or being used before it's valid.
- Signature panel: Should not show evidence of tampering. The panel should be signed and the signature should match your customer's signature on the sales slip.

Visa card features

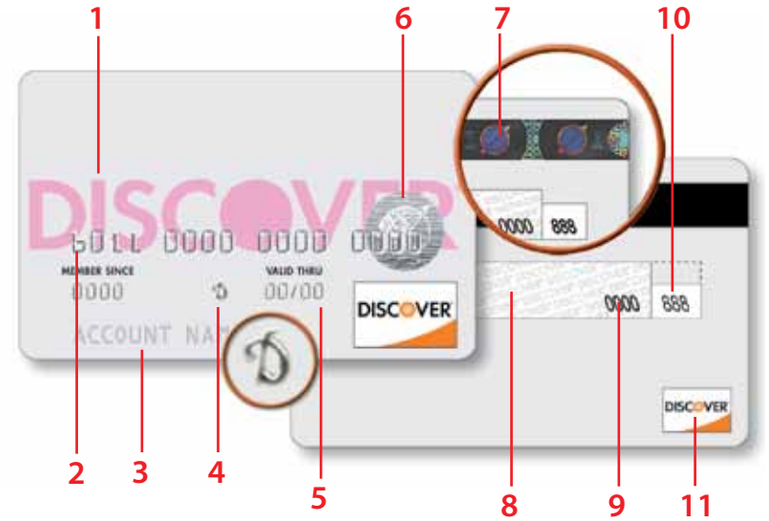
1. The signature panel must appear on the back of the card and contain an ultraviolet element that repeats the word "Visa." The panel will look like this one, or have a custom design. It may vary in length.
2. The Flying Dove Hologram appears on most cards, however its location on the card may vary. It can be on the front of the card, or a smaller hologram may be located on the back of the card.
3. The card may have a chip. Chip-enabled cards also have a magnetic stripe on the back.
4. All Visa embossed, unembossed or printed account numbers start with 4. All digits must be even, straight and of the same size.
5. The four-digit preprinted Bank Identification Number (BIN) must be printed directly below the account number and match the first four digits of the account number.
6. The magnetic stripe should be smooth and straight, with no signs of tampering.
7. The words "Authorized Signature" and "Not Valid Unless Signed" must appear above, below or beside the signature panel. If someone has tried to erase the signature panel, the word "VOID" will be displayed.
8. A three-digit Card Verification Value 2 (CVV2) must appear in the white box to the right of the signature panel or on the signature panel.
9. The Visa Brand Mark must appear on the card, in either the bottom right, top left or top right corner. A "V" is visible over the Brand Mark when the card is placed under an ultraviolet light.

MasterCard card features

1. All MasterCard account numbers start with 5. The embossing should be uniform in size and spacing, and extend into the hologram.
2. The preprinted Bank Identification Number (BIN) must match the first four digits of the embossed account number.
3. The valid date lists the last month in which the card is valid.
4. All new U.S.-issued consumer debit cards must display the Debit hologram. The three-dimensional hologram, which may appear on the front OR the back should reflect light and appear to move.
5. Issuers have the option of placing a holographic magnetic stripe on the card back, replacing the Globe hologram or the Debit hologram.
6. The magnetic stripe should appear smooth, with no signs of tampering.
7. The last four digits of the account number appear on the signature panel in reverse indent printing. The three-digit Card Verification Code 2 (CVC2) appears to the right of the signature panel.
8. The word "MasterCard" is printed repeatedly at an angle on a tamper-evident signature panel.

Discover Card features

1. "DISCOVER" or "DISCOVER NETWORK" will appear under an ultraviolet light.
2. All Discover account numbers start with 6. Embossed card numbers should be uniform in size and spacing, and extend into the hologram. Unembossed cards may display account number and expiration date printed flat on the front.
3. A business name may be embossed below the account name.
4. Embossed security character appears as a stylized "D." No stylized "D" appears on unembossed cards.
5. "Valid Thru" indicates the last month in which the card is valid.
6. All cards display a hologram on the card front with a globe pierced by an arrow, unless the card back displays a holographic magnetic stripe.
7. Newer cards display a three-dimensional holographic magnetic stripe which (when tilted) shifts color and appears to move.
8. "DISCOVER" or "DISCOVER NETWORK" appears on a tamper-evident signature panel.
9. The last four digits of the card number are displayed on the signature panel in reverse indent printing.
10. The three-digit Card Identification Data (CID) is printed in a separate box to the right of the signature panel on the card back.
11. The Discover or Discover Network acceptance mark will appear on the front AND/OR back of the card.



Discover and the Discover Acceptance Mark are service marks used under license from Discover Financial Services.

American Express Card features

1. All American Express® Card Numbers start with "37" or "34." The Card Number appears embossed on the front of the Card. Embossing must be clear, and uniform in sizing and spacing. Some Cards also have the Card Number printed on the back of the Card in the signature panel. These numbers, plus the last four digits printed on the Charge Record, must all match.
2. Preprinted Card Identification Numbers (CIN) must always appear above the Card Number, on either the right or the left edge of the Card.
3. Do not accept a Card outside the valid dates.
4. Only the person whose name is embossed on a Card is entitled to use it. Cards are not transferable.
5. The signature on the back of the Card must match the Cardmember's signature on the Charge Record, and must be the same name that appears on the front of the Card. The signature panel must not be taped over, mutilated, erased or painted over. Some Cards also have a three-digit Card Security Code (3CSC) number printed on the signature panel.

   Some Cards contain a holographic image on the front or back of the Card to determine authenticity. Not all American Express Cards have a holographic image.

What to do with an unsigned card

All card issuers require cardholders to sign their payment cards before use. Before accepting an unsigned card, you should:

- Ask for a photo ID* and compare the signature on it with the one on the sales slip.
- Record the number and expiration date of the ID (if local laws permit). (See General acceptance guidelines on p. 6.)
- Ask your customer to sign the card before completing the transaction, and compare with the signature(s) on the payment card sales slip and/or ID. If the customer refuses to sign the card, do not accept the card; refer your customer to the card issuer if he or she has questions.

Warning signs of card fraud

In addition to examining every card you accept, watch for other factors that can signal potential card fraud. One of the most common types of card fraud is unauthorized use of a lost or stolen card. Even if the cardholder has not yet reported the card missing, you can often prevent a fraudulent sale if you're alert to unusual customer behavior. Consider calling your telephone authorization number for a Code 10 (see p. 13) if your card customer:

- makes purchases without regard to size, color, style or price
- rushes, stalls or attempts to distract you as you complete the transaction
- says the magnetic stripe is damaged or worn and/or claims the card information must be manually entered on your terminal (see p. 15)
- purchases a large item (e.g., a refrigerator) and insists on taking it immediately rather than having it delivered — even when delivery is included in the price
- makes a purchase, leaves the store and then returns to make more purchases
- pulls the payment card from a pocket rather than a wallet
- signs the payment card sales slip in a deliberate or unnatural manner
- buys clothing without trying it on — or declines alterations even if they are included in the price
- makes a large purchase right at the last minute when the store is closing
- charges expensive items on a newly valid card
- cannot or will not present a photo ID — or provides a temporary ID with no photo*

Keep in mind that any of these circumstances can occur in a legitimate transaction. Use your best judgment. Let your instincts steer you and call for a Code 10 if you're unsure.

** You cannot refuse to honor a signed payment card solely because the customer will not provide photo ID or other personal information. If you are suspicious, call for a Code 10 (see p. 13).*

Code 10 procedures

If you're suspicious about a card transaction for any reason, hold the card in your hand, call your telephone authorization number and ask for a Code 10. A Code 10 signals potential fraud and will be handled by a specially trained operator to avoid alarming your customer. The operator may ask you a series of questions or talk directly with your customer to determine whether fraud may be involved. The operator will then provide a response code or instruct you to retain the card (see Recovering a payment card).

Recovering a payment card

When seeking authorization on a payment card transaction, you may be instructed not to return the card to your customer. This may mean that the card has been reported lost or stolen or that fraud has been detected. Follow your company's procedures and notify your supervisor. If you're told to retain the card or receive a "Pickup" message on your electronic terminal, hold the card in your hand and discreetly advise your customer of the situation. Use your best judgment to avoid any confrontation, but hold onto the customer's card if you think you can do so safely. Then call us or ask your telephone authorization center for instructions on how to turn in the card in accordance with the card issuer's requirements. Be sure to:

1. Keep a record of the card account number.
2. List the following information and turn it in to us with the card:
   - the card account number;
   - your business name and address;
   - the person who recovered the card; and
   - the reason for recovery (e.g., whether recovery instructions resulted from a normal authorization or a Code 10).

Card recovery rewards

You may receive a cash reward for properly recovering a payment card. Rewards are offered by payment card associations, card issuers and some merchants. Please call us if you'd like to know more about recovery rewards.

Turning in lost cards

If you find a lost payment card or a customer turns one in or leaves one behind, call us for instructions on how to turn it in to us.

Processing Transactions

Once you've checked to be sure the card is valid, the next stage is processing the transaction, and the first step in processing is getting authorization. To reduce your risk of chargebacks (see pp. 19–21), you must obtain authorization for every transaction. If you use an electronic authorization terminal, you'll complete authorization and processing in one step (see below). If your electronic terminal fails, refer to p. 16. To order a replacement terminal for your business, please contact your merchant representative.

Electronic processing

This is the fastest, safest and most accurate way to process payment card transactions. Follow the general procedures below, referring to the operating manual of your electronic terminal for more specific instructions. Hold the card in your hand until all steps are completed.

1. Swipe the card's magnetic stripe through the terminal. Some terminals may require you to key-enter the last four digits of the card account number or place an electronic payment card sales slip in the terminal's printer. If the terminal cannot read the magnetic stripe, or if you're processing a mail, phone or Internet order, or a recurring payment (see pp. 17–18), key in the information embossed on the card and, if the card is present, make a manual imprint of the card on a separate sales slip (see p. 16).
2. If the card is an online debit card your terminal will prompt you to have your customer enter his or her personal identification number (PIN).
3. If the card account number displays on the terminal screen, make sure it matches the account number embossed on the card. If it doesn't match, retain the card (see Recovering a payment card, p. 13).
4. Enter the transaction amount. Each transaction must be processed on a single sales slip.
5. One of the following response codes will be displayed on the terminal screen:
   - A number preceded by "Auth" or "Authorization" is an authorization code. This number should print out on the sales slip. Now proceed to Step 6.
   - "Call Center" or "Pickup" means there may be a problem with the card. Retain the card (see Recovering a payment card, p. 13).
   - "Decline" means the transaction cannot be authorized. Do not accept the card. Return it to your customer and discreetly advise that the card has been declined, and request another form of payment. If your customer has questions about the card being declined, refer him or her to the card issuer.
   - "Unknown card" and similar messages usually mean the card is of a type you are not set up to accept (see p. 5), or that there is a problem with the card or card account. Do not accept the card without telephone authorization.
6. Make sure all information is correct and legible on all copies of the sales slip. Do not circle the expiration date or obscure the printed information in any way.
7. Watch the customer sign the sales slip. Compare the signature with the one on the back of the card. If you can't tell whether they match, ask for a photo ID (see note on p. 13).
8. Return the card and customer copy of the sales slip to the customer. If you think the transaction may be fraudulent (even if you've received authorization) call for a Code 10 (see p. 13).

Processing key-entered transactions

It pays to swipe the stripe

On the back of every card, you'll find a magnetic stripe. It contains the cardholder name, card account number and expiration date, as well as special security information designed to help detect counterfeit cards. When the stripe is swiped through the terminal and electronically read, this information is relayed to the Issuer and used as crucial input to the authorization decision.

What happens with key-entered transactions

Sometimes when you swipe the card, the terminal is not able to read the magnetic stripe and perform an electronic authorization. In this situation, you may need to key-enter the transaction data. When transactions are key-entered, special security information benefits are not available.

Examples of legitimate reasons for key-entry:

- The card's magnetic stripe cannot be read (the stripe is damaged)
- A terminal is not available (home delivery)
- The card is not present (mail, telephone and Internet transactions)
  Note: you must be approved by us for card-not-present transactions.

Examples of situations causing unnecessary key-entry

- The terminal's magnetic stripe reader is not working properly
- The card is not being swiped properly through the terminal

Disadvantages of a key-entered transaction

- Increased risk of fraud and counterfeit: The magnetic stripe's special security features that work with your terminal and the authorization system are ineffective. This raises the risk of dispute or chargeback.
- Cost: Key-entered transactions cost more to process, and may be declined more often.
- Less efficient: Key-entered transactions are more time-consuming and allow more potential for error.
- Lost sales: Key-entered transactions may be declined more often, making the potential for lost sales higher.

Manual processing if a card's magnetic stripe isn't working

1. Take a look at the card's security features to make sure the card is not counterfeit or has not been altered in any way.
2. You may wish to ask for a photo ID. Please explain to your customer that this is for their protection.
3. Follow store procedures, which may require you to use the terminal's manual override feature to key-enter the transaction data for authorization.
4. Make sure to imprint the card on the transaction receipt. The imprint will prove the card is present in the event of a dispute, and minimize potential for financial liability.
5. Suggest to your customer that he/she note whether the stripe is working the next time the card is used. If transactions are being key-entered at other merchant locations, the customer may want to contact the card issuer for a replacement.

Telephone authorization and manual processing

If your electronic authorization terminal has failed, or if you receive a "Call Center" response from your terminal, call your telephone authorization number as part of the manual processing procedure. Follow the steps outlined below, holding the card in your hand until all steps are complete.

1. Make a card imprint on a manual sales slip using your card imprinter.
2. Fill in the transaction information (item description, amount, etc.). Each transaction must be processed on a single sales slip.
3. Call for authorization. You may be asked to provide:
   - your merchant ID number; and
   - the card account number, expiration date, Bank Identification Number and CVV2 (see p. 8), CVC2 (see p. 9), CID (see p. 10) or CIN (see p. 11); and
   - the amount of the transaction.

4. The operator will give you a response code (see Step 5 on p. 14) or provide other instructions. If the transaction is approved, write the authorization code in the space provided on the sales slip.
5. Make sure all information is correct and legible on all copies of the sales slip. Do not circle the expiration date or obscure the printed information in any way.
6. Watch the customer sign the sales slip. Compare the signature with the one on the back of the card. If you can't tell whether they match, ask for a photo ID (see note at bottom of p. 12).
7. Return the card and customer copy of the sales slip to the customer.
8. Manually enter the transaction to your electronic authorization terminal as an "offline" transaction when the terminal is functional.

If you think the transaction may be fraudulent (even if you've received authorization) call for a Code 10 (see p. 13).

Processing returns

Follow the guidelines below when completing refunds or exchanges on card purchases, referring to p. 14 for card processing instructions. You cannot refund cash on any card sale unless the customer has a gift receipt.

- If an even exchange is being made, no card processing steps are needed.
- If your customer exchanges a purchase for an item of greater or lesser value, process a credit voucher for the amount of the returned item, including tax. Then process a separate transaction for the new item.
- If your customer requests a refund with no exchange, process a credit voucher for the amount of the returned item, including tax.

To minimize customer disputes and chargebacks, you should post a clear return policy near your registers and within inches of the signature on the sales slip.

Processing mail, telephone and Internet orders

You must have a special written agreement with us to process payment card orders by mail, phone or Internet. Follow the instructions on pp. 14–15 to complete processing electronically making sure to:

1. Record any personal information you need (cardholder address, phone number, etc.) somewhere other than on the sales slip (see Protect your customers, p. 6).
2. Make a notation on the sales receipt, describing the type of transaction: "MO" for mail order, "TO" for telephone or "IO" for Internet order.
3. Ask the cardholder to read you the three-digit number that is printed near the right side of the signature panel on Visa, MasterCard and Discover Cards. On American Express Cards, this security feature is a four-digit number that appears on the front of the card above the embossed numbers.

Using Address Verification Service (AVS)

Address Verification Service is a preventive measure that should be utilized when processing phone, mail or Internet transactions. This is a card-fraud prevention tool that compares the billing address provided by the customer with the cardholder address listed in the card issuer's files. Please call us for details on using AVS.

Processing preauthorized orders or recurring payments

A preauthorized order is an agreement you make with your customer to charge a series of recurring payments to his or her payment card over a given period of time. Under your card acceptance agreement with us, a preauthorized order must be made in writing and signed by the cardholder, and copies of the order must be available to us on request. A recurring payment agreement need not be in any specific form, but it must specify all information necessary to process the transactions:

- date agreement was signed
- cardholder name
- card account number and expiration date
- amount of each transaction to be charged to the card
- number and frequency of charges to be made
- period of time during which the cardholder grants permission for charges to be made

You should obtain authorization (see pp. 16–17) for each recurring payment on the date that payment is to be made.

Touch-tone processing

Various Audio Response systems can be used for making your deposits. Because of the number of different systems available, you should contact your service provider for further information on ARU or "touch-tone" processing.

After the Sale

Closing out your electronic terminal

For card transactions processed electronically (see p. 14), you will complete a procedure called closing the batch to reconcile those transactions and prevent balancing and deposit errors. A batch represents all payment card transactions processed during a given period of time, generally one business day.

Follow the general guidelines below to close a batch. Refer to the operating manual for your electronic terminal for more specific instructions.

1. Use a calculator to manually total the sales slips and credit vouchers for the batch.
2. Display terminal totals by using the "Display Totals/Batch Inquiry" function.
3. Compare terminal totals with calculator totals. If out of balance, print list of terminal entries, compare entries to sales slips and make any necessary adjustments in terminal.
4. Use your electronic terminal to transmit batch information. Each time you close a batch, your terminal begins a new batch with the next transaction processed.

Adjustments to your account

Processing fees

Processing fees, also known as the "discount fee" and "interchange fee," will be charged at the end of each month. Processing fees will be charged to your account according to your current merchant contract.

The interchange fee represents a portion of the overall expense incurred to process your sales. This fee is passed on to you as part of your discount fee, and is forwarded to your customers' card issuers. Processing fees help cover the cost of underwriting, billing and funding a variety of services.

Plan ahead

Be sure there is enough money in your merchant account to cover transaction adjustments, processing fees and chargebacks. To prevent overdrafts, you should maintain a balance of at least twice your average sales slip amount plus your average monthly processing fees.

Chargebacks and retrievals

A chargeback is the reversal of a sale or credit that is a result of a dispute by a cardholder or the cardholder's bank. Disputed transactions are usually transmitted electronically from the cardholder's bank to our credit card center where we will review them for accuracy.

Some chargebacks require a preceding retrieval. Each chargeback reason has different requirements. Most chargebacks require documentation from the cardholder and/or the merchant. We will return chargebacks to the issuing bank if a credit refund was already processed for the transaction in question.

Merchants receive a Chargeback Adjustment Advice Letter along with any cardholder documentation required. The Adjustment Advice will contain reasons for the debit and a request for information that should be included if you want to make a rebuttal. Merchants need to respond quickly to the request for this information. We recommend that you provide a copy of the Adjustment Advice as a cover sheet with each rebuttal. Each rebuttal should be sent individually to the attention of Rebuttals. It can take up to 20 days for the Chargeback Department to review the rebuttal and prepare a response.

The most common reasons for chargebacks are as follows:

- No Response to Retrieval Request: All retrieval requests need to be fulfilled upon initial request. Once a chargeback has been issued for a non-receipt chargeback, all reversal rights are forfeited.
- Unauthorized Mail Order/Telephone Order Transaction: This chargeback is initiated when the cardholder denies that they authorized a sale by mail or telephone. A merchant takes these types of orders at their own risk and would be responsible for supplying proof that the order was actually placed. Because there are no signatures involved in these types of transactions, the merchant should keep all records of shipping to assist in proving the transaction was initiated by the cardholder.
- Duplicate Processing: This chargeback is initiated when a cardholder is charged two or more times for the same transaction, and only authorized one. In some cases, this chargeback may be reversed if the merchant can supply proof of more than one signed and authorized sales slip with different invoice numbers on each slip.
- Non-Receipt of Merchandise: The cardholder states that they authorized the sale and were billed for the item, but never received the merchandise. If the merchant can supply proof of a shipping receipt signed by the cardholder, there is a chance of having the chargeback reversed.
- Missing Signature/Missing Imprint (Unauthorized): If a sales slip is missing a signature or card imprint, the issuing bank has a right to chargeback this item. It is the responsibility of the merchant to ensure all sales slips are signed by the cardholder and the sales slip is imprinted or mag-swipe read with the cardholder number. The signature should be checked against the signature on the back panel of the card. Every key-entered transaction requires the imprint of the card, along with the signature of the cardholder and all other information related to the sale.

Tips to reduce chargebacks

- Always obtain a credit card imprint or swipe the card through the terminal.
- Always obtain a cardholder signature. (This signature may be on the sales draft or on a guest registration card, rental agreement, etc. Verify the signature and card number on the back of the credit card to the cardholder signature and card imprint obtained.)
- Always obtain an authorization. (If at any time you receive a negative response, do not attempt further authorizations. Request an alternative method of payment.)

Draft retrieval request

If a transaction is disputed, the cardholder's bank will electronically transmit a retrieval request to us. By means of the draft retrieval, we can better respond to the disputing bank or processor on your behalf. You will be asked to submit a copy of a sales draft for the disputed transaction. Make sure to maintain your records, because you must be able to supply the requested documents for any transaction that has taken place within the past 12 months.

Draft retrieval requests are sent to you via fax or mail. The card associations and Discover require that we supply a copy of the draft(s) to the cardholder's bank in a timely manner. If the retrieval request is sent to you by fax, four attempts will be made to fax you the request. If the fax transmission is not completed, the retrieval request will be sent via mail. If the retrieval request is mailed, only one request will be sent.

The five key elements which must be present on each retrieval are:

1. Merchant name (DBA) and location
2. Date of the disputed transaction
3. Dollar amount of the disputed transaction
4. Account number
5. Expiration date

Any other documentation you can provide about the disputed transaction may assist in resolving the cardholder's inquiry and prevent a chargeback. When you fax the retrieval documentation back to us, we recommend that you use a copy of the original retrieval request as a cover sheet. Each retrieval should be sent individually, and should be directed to the attention of Retrievals. Ensure that documentation is complete and legible to avoid a Notice of Invalid Retrieval Fulfillment letter, which is sent when additional information is needed. You can help reduce the probability of a chargeback by providing the requested documentation in a timely manner.

Definitions

Acceptance: The process by which a merchant allows a payment card to be used by a customer as a means of payment.

Acquirer/Acquiring Member: A member of MasterCard, Visa or Discover that maintains merchant relationships and receives all transactions from the merchant.

Address Verification Service: A payment card fraud prevention tool that verifies the cardholder's billing address in order to help combat fraud in card-not-present transactions.

Arbitration: The procedure a member can use to resolve a chargeback-related dispute between two members.

Authorization: The process by which a transaction is approved by the issuer based on the cardholder account status and available credit.

Authorization Code: The alpha/numeric code designed by the issuer, given to a sales transaction as verification that the sale has been authorized.

Bank Identification Number: A four-digit number printed (not embossed) above or below the card account number on the front of Visa, MasterCard and Discover Cards.

Batch: A term that collectively refers to all payment card transactions processed during a given period of time (see also **Batch Header, Closing the Batch**).

Batch Header: A form or electronic message used to summarize payment card sales slip amounts being deposited at a merchant's bank.

Card Account Number: A 16-digit number embossed on a payment card; indicates the credit account or debit account to which the card is linked.

Card Identification Data (CID): The three-digit number indent-printed after the card account number on the signature panel on Discover Cards.

Card Identification Number (CIN): The four-digit number printed on the front of American Express Cards, above the embossed account number.

Card Imprint: An image of a payment card's embossing obtained by using a payment card imprinter.

Card Issuer: The bank, credit union or other financial institution through which a cardholder obtains a card.

Card Validation Code 2 (CVC2): The three-digit number indent-printed after the card account number on the signature panel on MasterCard cards.

Card Verification Value 2 (CVV2): The three-digit number indent-printed after the card account number on the signature panel on Visa cards.

Cardholder: The person or entity whose name is embossed on a payment card and who is the holder or an authorized user of the card account linked to that card.

Chargeback: The reversal of a card transaction.

Chargeback Period: The number of calendar days during which the issuer has the right to charge the transaction back to the acquirer (may not exceed 120 days).

Chargeback Reason Code: A numerical code that identifies the specific reason for the chargeback.

Check Card : Another name for a debit card.

Closing the Batch: A process by which a merchant reconciles electronic payment card transactions processed during a given period of time.

Code 10: A code that allows a merchant to alert the telephone authorization center to a possible fraudulent transaction without alerting the cardholder.

Counterfeit Card: A fraudulently produced card, or a card that has been altered with fraudulent information.

Credit Card: A card that accesses a credit account.

Credit Voucher: A form used to process a refund on a sale originally paid for with a payment card.

Debit Card: A payment card that accesses a deposit account.

Draft Laundering: The prohibited practice of processing payment card sales slips on behalf of other individuals or businesses; also known as "factoring."

Draft Retrieval Request: The request for either an original or a legible copy of the transaction information document or substitute draft as identified in the electronic record.

Electronic Authorization Terminal: A computerized device used by a merchant to record payment card information by reading it from the card's magnetic stripe, and to obtain authorization via electronic messages rather than via telephone.

Embossed/Embossing: Terms that refer to the raised characters on the front of a payment card, including the cardholder name, card account number, expiration date or valid dates.

Expiration Date: The date embossed on a payment card indicating when the card is no longer valid (see also **Valid Dates**).

Factoring: See **Draft Laundering**.

Floor Limit: A maximum purchase amount that does not require the merchant to obtain telephone or terminal authorization.

Hologram: A reflective image that appears on payment cards that do not have a holographic magnetic stripe.

Interchange Fees: Fees set by the card-issuing bank that are passed on to the merchant.

Logos: Images of the card associations and/or Discover, that appear on the card.

Magnetic Stripe: The strip that appears on the back of payment cards; stores electronic data representing the card account number and other card information. Newer cards have a holographic magnetic stripe.

Manual Processing: The procedure by which a merchant completes a payment card transaction using an imprinter to record card information on a manual payment card sales draft.

Manual Sales Slip: A payment card sales slip designed to record a payment card transaction processed manually rather than electronically.

Merchant Account: A merchant's business checking account, to or from which all payment card transactions, adjustments and processing fees are credited or debited.

Merchant Agreement: A contract between a merchant and a merchant acquirer that entitles the merchant to accept cards.

Merchant ID Number: A number that a merchant acquirer assigns to a merchant under a merchant agreement.

Offline: An operating mode in which terminals are not connected to a central computer. Responses are governed by guidelines set by the issuer.

Online: An operating mode in which terminals are connected to a central computer and have access to the database for authorizations, questions and file changes.

Payment Card: A financial transaction card issued by a financial institution.

Personal Identification Number (PIN): A security code entered by the cardholder during processing of an online debit card transaction.

Point of Sale (POS): The merchant location from which a customer makes a purchase.

Preauthorized Order: A cardholder's written authorization to process one or more recurring payments on his or her card account at a future date.

Processing: The procedure by which a merchant completes a payment card sales slip with details of a payment card transaction.

Processing Fees: Fees assessed to the merchant for authorization and settlement of card transactions.

Rebuttal: A notice a merchant files with the merchant acquirer to challenge a chargeback.

Recurring Payment: Payment card transactions processed under a preauthorized order.

Re-embossed: Altered by flattening embossed characters and embossing new characters in their place.

Response Code: A message returned through the authorization process that tells the merchant how to proceed with processing a payment card transaction.

Retrieval Request: The request for either an original or a legible copy of the transaction information document or substitute draft as identified in the electronic record.

Sales Slip: A form used to process a purchase paid for with a payment card.

Security Character: A unique character embossed on some Visa, MasterCard and Discover Cards.

Settlement: The process by which the amount of a payment card transaction is credited to or debited from a merchant account and card account.

Signature Panel: A strip on the back of every valid payment card where the cardholder signs the card.

Split Sale: A prohibited practice of dividing the dollar amount of an individual sale whether on the same card or placing it on a second card number to avoid obtaining an authorization for the "total" dollar amount of the original sale.

Support Documentation: The forms necessary to effect a chargeback transaction including any documentation received to substantiate the chargeback.

Surcharge: A dollar amount, added to the total price of a card transaction to cover the merchant's cost of processing. This practice is prohibited by the card associations and Discover.

Transaction: Any action between a cardholder and a member that results in activity on the account such as a purchase, cash balance, debit or credit adjustment.

Valid Dates: The dates embossed on a payment card indicating the time period during which the card may be used and accepted for payment (see also **Expiration Date**).