DISCLAIMER: This guide provides information on payment card industry guidelines for card acceptance, processing, mandated rules and regulations, and compliance for payment processing. Bankers' Bank of the West is not liable for any incorrect or outdated information contained in this document, and Bankers' Bank of the West is not responsible for any industry updates or changes not included in this guide. It is the responsibility of the merchant to understand and adhere to all payment industry card acceptance practices, rules and regulations that can be found on each Card Associations' website.

Last updated 11/2023

Important Information

Voice Authorization: 1-800-228-1122

To verify with the Card Issuing Bank, call:

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

Merchant Guide to Card Acceptance

What is in this Guide

Payment acceptance is an essential part of your business. This information guide reviews the steps that you will need to take to ensure customers are informed of their payment options and understand the terms of the sale. This guide will help you take full advantage of the benefits of accepting credit and debit cards for payment and includes tips and important reminders for validating cards to reduce the risk of fraud. It explains acceptance, processing procedures and requirements, and offers tips to help you optimize your profits from card sales.

This guide is part of your Merchant Services Agreement with your Merchant Provider. To remain in compliance with that Agreement and retain your card acceptance privileges, you must follow the industry rules, requirements, and regulations.

How to use this Guide

The Table of Contents on p. 2 lists topics covered in this guide and the Definitions section starting on p. 19 is where you will find definitions for the terms that appear in this guide.

Table of Contents

Card Basics

How cards work

Credit and debit cards issued by Financial Institutions are a convenient alternative to cash and checks. Mastercard, Visa, Discover, and American Express cards are accepted by millions of merchants worldwide. Payment cards are generally issued by a bank, credit union, or other Financial Institution.

Payment cards include both credit cards and debit cards. A credit card accesses a revolving credit account. A debit or prepaid card accesses funds in a deposit account (checking account) or a stored value or prepaid account with a specific balance.

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

Issuance

To issue Mastercard, Visa, Discover, or American Express cards, a Card Issuing Bank must first enter into a membership agreement with one or more of the Card Associations. Most Card Issuing Banks offer Mastercard, Visa, and Discover cards. American Express issues cards either directly to consumers, businesses or through Global Service Network Partners. To obtain a credit or debit card, a customer opens a deposit or credit account with a Card Issuing Bank or purchases a stored value or prepaid debit card. Your customer may have cards from several different Card Issuing Banks.

Acceptance

Your Merchant Services Agreement with your Merchant Provider specifies which cards you can accept. This may include Mastercard, Visa, Discover, American Express, or other. Details of the acceptance process can be found below.

Settlement

You receive payment for transactions you accept through a process called settlement. When your customer uses a card at your business, the Card Issuing Bank pays you on behalf of your customer via a credit posted electronically to your bank account. The Card Issuing Bank then bills your customer. For most transactions, that is all there is to it. Occasionally, processing errors or customer questions about a transaction may occur. More information on how such errors and questions are managed can be found within this guide.

Accepting Cards

Which cards can you accept?

Your Merchant Provider specifies which card types you should honor. You can accept them with confidence when you follow the directives in this guide. In addition to Visa, Mastercard, Discover, and/or American Express credit cards, your customers may present any of the following:

Mastercard, Visa, Discover, and American Express debit cards — Debit cards resemble Visa, Mastercard, Discover, and American Express credit cards (see pp. 7 - 10). Most Mastercard debit cards will have a unique debit hologram, while some will have the word "Debit" printed on the card. Most Visa debit cards will have the word "Debit" printed on the card. On Discover debit cards, the word "DEBIT" may appear anywhere within the gray shaded area on the card. American Express should have the word "DEBIT" printed on the card.

Debit cards may be authorized using offline (signature-based) or online (PIN-based) systems. Online debit cards are authorized through the debit card networks for funds availability and require entry of a Personal Identification Number (PIN). Offline debit cards process like a credit card.

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 your card processing solution allows for international cards. As a U.S. merchant, all payment card transactions accepted are processed in U.S. funds. Conversion differences are applied to cardholder accounts without affecting the cash value to you.

Other types of cards — There are a wide variety of other card types in today's marketplace. Stored value or prepaid 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 all credit and debit cards (see pp. 6 - 10).

Use of Payment Network brands

DO:

- Do prominently display relevant trademarks of the Payment Networks at each of your locations, in catalogs, on websites, and on other promotional material.
- Do only use the official trademarks of the Payment Networks in the official format.

DO NOT:

- Do not indicate that your Merchant Provider or any Payment Networks endorse your goods and/or services.
- Do not use the trademarks of any Payment Network after your right to accept the cards of that Payment Network has ended, or if that Payment Network has notified you to stop use of their trademark.
- Do not use the trademarks of the Payment Networks in any way that injures or diminishes the goodwill associated with the trademarks.
- Do not use the trademarks of the Payment Networks in any manner, including in any advertisements, displays, or press releases without prior written consent.

General acceptance guidelines

Point-of-Sale (POS) reminders

You must clearly and conspicuously:

- Divulge all material terms of sale prior to obtaining an authorization.
- Disclose any compliant discount or incentive for customers to pay with cash, check, credit, or debit card. Any such discount/incentive must be offered to all customers with no special treatment for any Payment Network or Card Issuing Bank.
- If you limit refund/exchange terms or impose other specific conditions for card sales, you must compliantly print the words "No Exchange, No Refund" on sales draft.

If you accept orders via the Internet, your website must include the following information:

- A complete description of the goods and services offered.
- Details of your 1) delivery process, 2) consumer data privacy policy, 3) cancellation policy, and 4) return policy.
- The customer service contact information, including email and telephone number.
- Your address, including your country.
- The transaction security used on your website.
- Any applicable legal restrictions.
- Your identity at all points of interaction with the cardholder.
- The date on which any free trial period ends.

Validating Card Present (CP) transactions where the cardholder/card is present

DO:

- You may request to check the card if the cardholder is present at the point-of-sale (POS).
    - Verify the card is legitimate and valid (see Card Identification Features section pp. 6 - 10).
    - Confirm the card is not visibly altered or mutilated.
    - Check the card's "valid from" date (if applicable) and the expiration date.
    - Validate the card number on the card is the same as the transaction receipt, if applicable.
    - Substantiate the name on the front of the card is the same on the transaction receipt, if applicable.
- Capture card data using the POS device by tapping/waving the card (contactless), inserting the card (chip card/ EMV), or swiping the card (magnetic stripe).
- Ensure that the cardholder enters their PIN using the keypad, if applicable and if prompted, or is allowed to bypass the PIN entry, if applicable.

Validating Card Not Present (CNP) transactions where the cardholder is not present at the point-of-sale

DO:

- Obtain the card account number, name as it appears on the card, expiration date, and the cardholder's billing address.
- Use the Address Verification Services (AVS), when applicable.
- Clearly print the following on the sales draft and provide a copy to the cardholder at the time of delivery:
    - The last 4 digits of the cardholder's account number.
    - The date of the transaction.
    - A description of the goods and/or services.
    - The amount of the transaction (including shipping, handling, etc.).
    - The cardholder's name, billing address, and shipping address.
    - The authorization code.
    - Your name and address (city and state required).
- Obtain proof of delivery of the goods and/or services to the address designated by the cardholder.
- Notify the cardholder of delivery time frames, special handling, and cancellation policies.
- Ship goods within 7 days from the date on which authorization was obtained. If the delivery is subject to delays (for example, out of stock) after the order has been taken, notify the cardholder and obtain fresh authorization of the transaction.
- Provide at least 1 month's prior written notice to your Merchant Provider of any change in your internet address.

DO NOT:

- Do not submit a transaction for processing until after the goods have been shipped or the service has been provided to the cardholder. The only exception to this is where the goods have been manufactured to the cardholder's specifications and the cardholder has been advised of the billing details.
- Do not accept card account numbers by electronic mail.
- Do not require a cardholder to complete a postcard or other document that displays the cardholder's account number in clear view when mailed or send any mailing to a cardholder that displays personal information in clear view.

Authorizations

- You must obtain an authorization approval code on ALL transactions.
- A positive authorization response remains valid (affecting the cardholder's available credit or available funds) for a timeframe set by the Card Issuing Bank or Card Associations, typically 8 to 10 days.
- An authorization approval code only indicates the availability of funds on an account at the time the authorization is requested. It does not indicate that the person presenting the card is the rightful cardholder nor is it a promise or guarantee that you will not be subject to a chargeback.
- You must not attempt to obtain multiple authorizations for a single transaction. If the sale is declined, request another form of payment.

Surcharging

A surcharge is a fee that a merchant adds to a credit card payment transaction (as a percentage of the sale) to cover the cost of processing the payment. The Card Associations and government entities such as states or local municipalities that allow surcharging have individual rules and regulations surrounding compliant surcharging. Check with your Merchant Provider to inquire if they have a compliant surcharge program in place. Some examples of the requirements for U.S. merchants that intend to surcharge are:

- Ensure all Card Associations (Mastercard, Visa, Discover, and American Express), local, state, and federal requirements and guidelines related to surcharging are followed. This may include notification to the Card Associations and your Merchant Provider at least 30 days in advance of beginning to surcharge.
- Limit surcharging to credit cards only *(surcharging is not allowed on debit and prepaid cards*) and to the maximum allowed for a credit card surcharge set by the Card Associations and government entities when applicable.
- Disclose and display the surcharge as required by the Card Associations and government entities per specific requirements such as but not limited to signage and receipt information disclosure.

Minimum Sales Amount

U.S. merchants may establish a minimum sale amount of up to $10 on credit card sales, but not on debit or prepaid card sales. Merchants are not allowed to place a maximum amount on card transactions, except when the Issuing Bank or Merchant Provider has not provided a positive authorization response for the transaction.

Split Sales

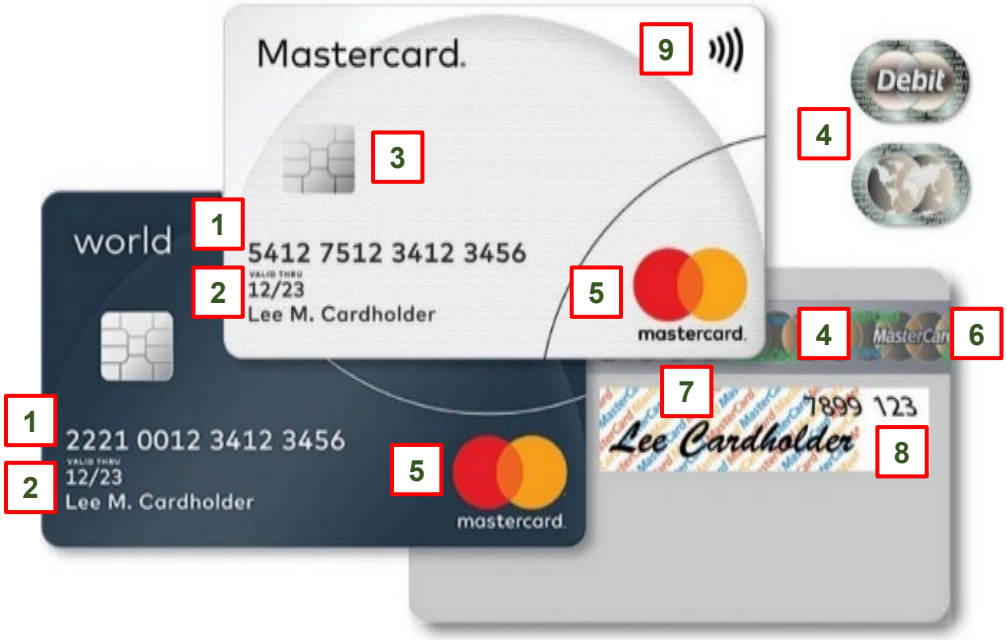
Do not process split sales. Attempting to avoid authorization (required on all transactions) by processing partial transaction amounts on separate sales slips is prohibited by the Card Associations and may result in chargebacks.

Card Identification Features

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. 16). Note: Some features pictured in this guide are optional and may not appear on all valid cards. Some cards may have the card number printed on the back of the card.

Mastercard card features

1. The account number must start with a 5 or a 2. The numbers should be uniform in size and spacing.
2. An expiration date must be present on the card.
3. Most cards will have an embedded chip.
4. One or more of the following holograms must be present on the card:
   - Mastercard Global Hologram must be on the card front or back in either gold or silver.
   - Debit Mastercard Hologram must be on the card front or back in either silver (in the U.S. or other debit card countries) or copper (in the U.S. only).
   - Mastercard HoloMag — a holographic magnetic stripe may appear in place of or in addition to the Mastercard Global Hologram or Debit Mastercard Hologram.
   - The hologram should reflect light and appear to move when tilted.
5. The Mastercard brand mark must be present on the card.
6. The card must have either a magnetic stripe or a Mastercard HoloMag. The stripe should be smooth and straight with no signs of tampering.
7. The tamper evident Mastercard Signature Panel must be present, must not show evidence of tampering, and must contain the cardholder's signature.
8. The last four digits of the account number may appear in the upper right corner of the Mastercard signature panel. The 3-digit Card Validation Code (CVC) must be printed to the right of the Mastercard signature panel.
9. Contactless indicator will appear on cards equipped with RFID or NFC.



Visa card features

1. The magnetic stripe should be smooth and straight with no signs of tampering.

2. 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. 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.

3. The mini dove design hologram may appear on the back either below or to the left of the signature panel. The three-dimensional dove hologram should appear to move as you tilt the card. If you do not see a mini dove on the back of the card, check for the traditional dove hologram above the Visa brand mark on the front of the card.

4. Chip cards contain a small, embedded microchip that is virtually impossible to copy or counterfeit.

5. Embossed, unembossed, or printed account number on valid cards begins with a 4. All digits must be even, straight and the same size. Printed card numbers will appear on either the front or back of the card.

6. Card Verification Value (CVV) is a 3-digit code that appears either in a white box to the right of the signature panel or directly on the signature panel. Portions of the account number may also be present on the signature panel.

7. Contactless indicator will appear on cards equipped with RFID or NFC.

8. Expiration or "Good Thru" date should appear below the account number.

9. Visa brand mark must appear in either the bottom right, top left, or top right corner. An ultraviolet "V" is visible over the Visa brand mark when placed under an ultraviolet light.

Discover card features

1. The card may be a chip-enabled card, which will also have a magnetic stripe on the back.
2. Card numbers will appear on either the front or back of the card. Card numbers begin with the number 6 and are composed of 16 digits that should be clear and uniform in size and spacing.
3. The "Valid Thru" date may appear on either the front or back of the card in MM/YY format that indicates the last month in which the card is valid.
4. The cardholder's name and, if applicable, business name, will appear on either the front or back of the card.
5. Cards must contain either the holographic magnetic stripe on the back of the card OR the security hologram on the card front or the card back.
6. The words "DISCOVER" or "DISCOVER NETWORK" appear on a signature panel on the back of the card. An underprint of "void" becomes visible if erasure of the signature is attempted.
7. The Discover acceptance mark will appear on the back of most cards and may also appear on the front of the card along with other affiliated logos.
8. A 3-digit Card Verification Value (CVV) will appear to the right of the signature panel.

Features on Discover Debit, Private Label, and Prepaid cards may differ from those shown here.

American Express card features

1. 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. Prepaid cards may not have a cardmember name on the card. The signature panel must not be taped over, mutilated, erased, or painted over. Some cards also have a 3-digit Card Security Code (CSC) number printed on the signature panel.

2. Some cards have an embedded chip on which data is stored and used to conduct a charge.

3. All American Express card numbers start with a 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.

4. Do not accept a card outside the valid dates.

5. Only the person whose name appears on an American Express card is entitled to use it. Cards are not transferable.

6. A preprinted Card Identification Number (CID) must always appear above the card number on either the right or the left edge of the card.

Card features not shown here may appear on some cards.

- Some cards have a holographic image on the front or back of the card to determine authenticity. Not all American Express cards have a holographic image.
- Prepaid cards may have the name and numbers printed rather than embossed. The cardmember name may be "Recipient" or "Traveler."

Processing Transactions

Once you have checked to be sure the card is valid, the next stage is processing the transaction. The first step in processing is obtaining an authorization. To reduce your risk of chargebacks (see pp. 18 – 19), you must obtain authorization for every transaction. If you use an electronic device, you will complete authorization and processing in one step (see below). If your electronic device fails, please contact your Merchant Provider for a replacement.

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 payment device for more specific instructions. Steps may be completed by merchant or cardholder, depending on the environment.

1. Instruct the customer to insert their card into the payment device. The customer may also tap their card, phone, or other mobile device near the card reader for a contactless payment (see p. 12) or swipe the card if it does not have a chip. If your payment device cannot read the card's information, or if you are processing a mail, phone or Internet order, or a recurring payment (see p. 13), key in the information from the card.

2. Depending on how your payment device is set up, you may be prompted to have your customer enter their Personal Identification Number (PIN) if the card is a debit card.

3. If the card account number displays on the payment device, make sure it matches the account number embossed or printed on the card.

4. Enter the transaction amount.

5. One of the following response codes will be displayed on the payment device:
   - A number preceded by "Auth" or "Authorization" is an authorization code. This number should print 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. 17).
   - "Decline" means the transaction cannot be authorized. Do not accept the card. Return it to your customer and discreetly advise them that the card has been declined. Request another form of payment and instruct the customer to contact their Card Issuing Bank with questions.
   - "Unknown card" and similar messages usually mean the card is of a type you are not set up to accept (see pp. 3) 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. 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. 16).

No signature required on chip card transactions

Mastercard, Visa, Discover, and American Express no longer require U.S merchants to collect a signature during a chip card transaction. Chip cards are nearly impossible to counterfeit because the chip generates a one-time-use code each time the card is used, making it unnecessary to compare signatures.

Unembossed cards

Cards that have the account number, expiration date, and cardholder name printed rather than embossed should be accepted if all the card security features are present. As with all other card transactions, if any of the security features are missing or altered, call for a Code 10 authorization (see p. 16).

Processing mobile payments

Mobile commerce has become as significant as plastic cards were a few decades ago, and it is embraced by many consumers as their payment method of choice. Mobile payments are transacted by customers using their mobile device rather than payment cards, checks, or cash. As smart devices are now more commonplace, consumers routinely use them to browse merchandise and transact business.

Smart devices can also be used by merchants to accept payments. Merchants are encouraged to incorporate this technology into their payment platform.

Contactless payments 

Many payment cards, smartphones, and other smart devices are equipped with radio frequency identification (RFID) or near field communication (NFC), which enables the devices to transmit payment information simply by being held near the card reader. Contactless cards display a symbol like the one pictured above.

Rather than inserting the card's chip into the reader, the customer taps their card or mobile device in close proximity of the card reader. Payment information is securely sent to your payment device to process the transaction.

Contactless payments offer benefits to both merchants and cardholders. Transaction times are reduced, which can speed up your checkout line.

Telephone authorization and manual processing

If your payment device has failed to authorize a transaction, or if you receive a "Call Center", "Call", or "Call Hold" response from your payment device, 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. Ensure you obtain the following information:

   - Card account number
   - Cardholder name as it appears on the card if present.
   - Expiration date as it appears on the card.
   - Cardholders billing address (the address that appears on the billing statement).
   - Shipping address (if applicable, the address where the merchandise will be shipped which may be the same as the billing address).
   - The Card Verification Value/Code (CVV, CVC), a 3-digit code for Mastercard, Visa, and Discover (4-digit number for American Express) which is not a part of the card number and is typically printed on the back of the card (usually in the signature panel).

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 or account number.
   - The amount of the transaction.

   The operator will give you a response code (see Step 5 on p. 11) or provide other instructions. If the transaction is approved, write the authorization code in the space provided on the sales slip.

4. 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.

5. Return the card and customer copy of the sales slip to the customer.

6 Manually enter the transaction to your payment device as an "offline" transaction when the device is functional. Entry of "offline" or "forced" transaction may require the use of a password.

If you think the transaction may be fraudulent (even if you have received authorization), call for a Code 10 (see p. 16).

Processing mail, telephone and Internet orders

You must have a special written agreement with your Merchant Provider to process payment card orders by mail, phone, or Internet. Make sure to:

1 Record any personal information you need (cardholder address, phone number, email address, time and date of the order, details of the conversation, etc.) somewhere other than on the sales slip (see "Protect your customers,"p. 15). You should always keep copies of the order forms and obtain proof of delivery of merchandise to the address specified by the cardholder.

2 Make a notation on the sales receipt, describing the type of transaction: "MO" for mail order, "TO" for telephone order, or "IO" for Internet order.

3 Ask the cardholder to read you the 3-digit number that is printed near the right side of the signature panel on Mastercard, Visa, and Discover cards. On American Express cards, this security feature is a 4-digit number that appears on the front of the card above the printed numbers.

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 the payment card over a given period of time. Under your Merchant Services Agreement with your Merchant Provider, a preauthorized order must be made in writing and signed by the cardholder, and copies of the order must be available 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 for each recurring payment on the date that payment is to be made.

Processing key-entered transactions

The EMV chip is essentially a tiny computer that is extremely hard to counterfeit. The chip encrypts bank information during transmission, making it even more secure than magnetic stripe cards. Most payment cards will also have a magnetic stripe. It would contain the cardholder's name, card account number, and expiration date, as well as special security information designed to help detect counterfeit cards. When the magnetic stripe is swiped through the payment device and electronically read, this information is relayed to the Card Issuing Bank and used as crucial input to the authorization decision.

What happens with key-entered transactions?

Sometimes when a card is inserted or swiped, the payment device is not able to read the card's information to 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 EMV chip has malfunctioned.
- The card's magnetic stripe cannot be read (the stripe is damaged).
- A payment device is not available; for example, merchant is using virtual terminal (computer) for processing.
- The card is not present (mail, telephone, and Internet transactions). Note: You must be approved by your Merchant Provider for card-not-present transactions.

Examples of situations causing unnecessary key-entry

- The payment device's chip card or magnetic stripe reader is not working properly.
- The card is not being inserted or dipped properly into the payment device.

Disadvantages of a key-entered transaction

- Increased risk of fraud and counterfeit: The card's special security features that work with your payment device and the authorization system are ineffective. This raises the risk of dispute or chargeback.
- Cost of a transaction: 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 chip or magnetic stripe is not working

1. Check the card's security features to make sure the card is not counterfeit or has not been altered in any way.
2. You may 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 payment device's manual override feature to key-enter the transaction data for authorization.
4. Suggest to your customer that they note whether the chip or stripe is working the next time the card is used. If transactions are key entered at other merchant locations, the customer may want to contact the Card Issuing Bank for a replacement.

Processing returns

Follow the guidelines below when completing refunds or exchanges on card purchases. You should not 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. The same card that was used in the original sale transaction should be used for the refund transaction.
- 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 on the sales slip.

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 Services 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 your Merchant Provider and to the U.S. Secret Service.

Data Security and Fraud Prevention

The Payment Card Industry Security Standards Council (PCI SSC) comprised of the Card Associations (Mastercard, Visa, Discover, and American Express) developed and enforces the industry security standards, rules, and regulations. The official website is https://www.pcisecuritystandards.org/. With the explosive growth of identity theft, data security has become more than just important — it is mandatory. In an effort to slow the continued growth of fraud and identity theft, Mastercard, Visa, Discover, and American Express have collaborated in creating a worldwide standard for consumer data protection.

The result is a global data security standard called the Payment Card Industry Data Security Standard (PCI DSS). 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 to complete and pass a Self-Assessment Questionnaire (SAQ) on an annual basis and to adhere to the PCI DSS requirements outlined below. Your Merchant Provider will supply you with details on SAQ completion and compliance assistance. You have agreed to adhere to this requirement as per your Merchant Services Agreement.

PCI DSS Requirements and Security Assessment Procedures

- Install and maintain a firewall configuration to protect data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored data.
- Encrypt transmission of cardholder data across open, public networks.
- Protect all systems against malware and regularly update anti-virus software or programs.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need-to-know.
- Identify and authenticate access to system components.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security for all personnel.

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. 12) 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.

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 Issuing Bank's files.

AVS does not guarantee against chargebacks, however if used properly, it assists you in reducing the risk of fraud by confirming whether certain elements of the billing address provided by your customer match the billing address maintained by the Card Issuing Bank. AVS is a separate process from obtaining an authorization and will provide a separate response.

Warning signs of card fraud

In addition to examining every card that is presented to you for payment, 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 are alert to unusual customer behavior.

Consider calling your telephone authorization number for a Code 10 (see below) 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 chip or magnetic stripe is damaged and/or claims the card information must be manually entered on your payment device (see p. 14).
- 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 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. You cannot refuse to honor a signed payment card solely because the customer will not provide photo ID or other personal information.

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 are unsure (see "Code 10 procedures" below).

Code 10 procedures

If you are 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 (see above). 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" below).

What to do with an unsigned card

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

- Record the number and expiration date of the ID (if local laws permit).
- Ask your customer to sign the card before completing the transaction and compare with the signature on the payment card sales slips and/or ID. If the customer refuses to sign the card, do not accept the card. Refer your customer to the Card Issuing Bank if there are any further questions.
- Ask for a photo ID and compare the signature on it with the one on the sales slip. You cannot refuse to honor a signed payment card solely because the customer will not provide photo ID or other personal information.

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 are told to retain the card or receive a "Pickup" message on your payment device, 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 your Merchant Provider or ask your telephone authorization center (see p. 1) for instructions on how to turn in the card in accordance with the Card Issuing Bank's requirements.

Be sure to:

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

After the Sale

Settling your payment device transactions

For card transactions processed electronically (see p. 11), 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. Some payment devices or solutions are set up to close out/batch automatically at a specified time each day.

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

- Use a calculator to manually total the sales slips and credit vouchers for the batch.
- Display payment device totals by using the "Display Totals/Batch Inquiry" function.
- Check for errors, discrepancies, or other verbiage that indicates the batch did not successfully close.
- Compare payment device totals with calculator totals. If out of balance, print list of payment device entries, compare entries to sales slips and make any necessary adjustments in payment device.
- Use your payment device to transmit batch information. Each time you close a batch, your payment device begins a new batch with the next transaction processed.

Note: You must close batches daily in a timely manner to avoid higher processing fees and potential chargebacks.

Adjustments to your account

Processing fees

Processing fees along with monthly service fees will be charged at the end of the month to your bank account according to your current Merchant Services Agreement.

Plan ahead

Be sure there are enough funds in your bank account to cover transaction adjustments, processing/monthly 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/monthly fees.

Chargebacks and retrievals

A chargeback is the reversal of a sale that is a result of a dispute by a cardholder or the cardholder's bank (Card Issuing Bank). Disputed transactions are usually transmitted electronically from the cardholder's bank to the credit card center where they are reviewed for accuracy. Some chargebacks require a preceding retrieval (request for a copy of a sales receipt). Each chargeback reason has different requirements. Most chargebacks require documentation from the cardholder and/or the merchant.

Merchants receive a Chargeback Adjustment Advice via email 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 submit a rebuttal. Follow the instructions in the Chargeback Adjustment Advice and always respond quickly to the request for this information as there is typically a deadline to submit a rebuttal. It is recommended that you provide or use a copy of the Chargeback Adjustment Advice as a cover sheet with each rebuttal. It can take up to 20 days for the Chargeback Department to review the rebuttal and prepare a response. Be sure to maintain a valid email address on your Merchant Account as timeliness is critical in the chargeback process.

The most common reasons for chargebacks are as follows:

Chargebacks can occur for a variety of reasons, including fraudulent use of a credit card, dissatisfaction with service or merchandise, and duplicate charges.

- **Criminal Fraud:** When a stolen card is used to make a purchase.
- **Merchant Error and/or Service Error:** When the business makes a clerical error, such as a duplicate charge or incorrect billing amount, or when a company has an inadequate return policy, misrepresents their products, or its services were not fully delivered to their client's satisfaction.
- **Cardholder Initiated:** When a customer has buyer's remorse and changes their mind or does not recognize the charge on their billing statement due to the payment descriptor or difference in currency.

Tips to reduce chargebacks

1. Always process the card through your payment device.
2. Always obtain an authorization.
3. Always close out/batch payment device daily/timely to avoid chargebacks due to delayed presentment (see p. 17).
4. Honor declined response on transaction attempt. Do not attempt to split sales or circumvent card, transaction or daily transaction or amount limits. Do not attempt further authorizations and request an alternative method of payment, if needed.
5. If a refund needs to be processed, issue a credit to the cardholder on the same account as the purchase in a timely manner.
6. Do not issue a credit to the cardholder in the form of cash, check, or in-store merchandise credit as you may not be able to recoup the funds in the event of a chargeback.
7. For recurring transactions, ensure customers are fully aware of the conditions:

    - Cancel recurring transactions as soon as notification is received from the cardholder and issue the appropriate credit as needed to the cardholder in a timely manner.
    - Notify the cardholder within 10 days in advance of each billing to allow the cardholder time to cancel the transaction.
    - Provide proper disclosure of your refund policy for returned/cancelled merchandise or services to the cardholder at the time of the transaction.
    - Ensure delivery of the merchandise or services rendered to the cardholder.

Draft retrieval request

If a transaction is disputed, the cardholder's bank may electronically transmit a retrieval request. You may be asked to submit a copy of a sales draft for the disputed transaction or your Merchant Provider may process this request automatically. 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. By responding to the draft retrieval promptly, you enhance the dispute resolution process on your behalf.

Draft retrieval requests are sent to you via email. The Card Associations require a copy of the draft(s)/sales receipt(s) to fulfill the request from the cardholder's bank in a timely manner. If the retrieval request is sent to you by fax transmission, four attempts will be made. If the email or fax transmission is not completed, the retrieval request will be sent via postal mail. If the retrieval request is mailed, only one request will be sent.

The five key elements that must be present on each retrieval request 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 or Card Issuing Bank's inquiry and prevent a chargeback or entering into Arbitration. When you submit the required documentation by email or fax, follow the instructions on the retrieval request. It is recommended that you provide or use a copy of the original retrieval request as a cover sheet. Ensure that documentation is complete and legible to avoid a Notice of Invalid Retrieval Fulfillment Advice, 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. Be sure to maintain a valid email address on your Merchant Account as timeliness is critical in the retrieval process.

Definitions

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

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

Arbitration: The procedure a merchant can use to resolve a chargeback-related dispute.

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

Authorization Code: The alpha/numeric code given to a transaction by the Card Issuing Bank as verification that the transaction has been authorized.

Back-End Processing Platform: Where the Merchant Account resides. Settles/funds merchant transactions, deposits, and routes transactions through the Card Networks / Debit Networks to the Card Issuing Bank (cardholder statement).

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

Bluetooth: A short-range wireless technology standard that is used for exchanging data between fixed and mobile devices.

Bring Your Own Device (BYOD): The growing trend of merchants providing their own smart devices (phones, tablets, etc.) for credit card processing purposes.

Buy Now/Pay Later (BN/PL): A type of financial loan arrangement defined by a third party. This is different than an installment or recurring payment.

Card Account Number/Primary Account Number (PAN): A 15 or 16-digit number embossed or printed on a payment card, indicating the credit account or debit account to which the card is linked.

Card Associations/Card Brands/Card Networks: Card Associations/Brands include Mastercard, Visa, Discover, and American Express. Card Networks are the Card Associations/Brands' systems for routing credit and signature-based debit transactions from the Merchant Acquirer to the Card Issuing Bank (cardholder statement).

Card Identification Number (CID): The 4-digit number printed on the front of American Express cards above the account number.

Card Imprint: An image of a payment card's embossing obtained by using a Card Imprinter/Manual Card Imprinter device. Mostly outdated as many cards have unembossed information and can no longer be imprinted due to the lack of embossing.

Card Issuing Bank: The bank, credit union, or other Financial Institution through which a cardholder obtains a card.

Card-Not-Present (CNP) Transaction: A credit or debit card purchase made by phone, mail, Internet, or mobile device in which the physical card is not inserted or swiped through an electronic payment device.

Card Validation Code (CVC): The 3-digit number printed after the card account number on the signature panel on Mastercard cards.

Card Verification Value (CVV): The 3-digit number printed after the card account number on the signature panel on Visa and Discover cards.

Cardholder: The person or entity whose name is embossed or printed 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, typically initiated from a cardholder dispute.

Chargeback Period: The number of calendar days during which the Card Issuing Bank has the right to charge the transaction back to the Merchant 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.

Chip-and-PIN: The method of processing a transaction in which the customer enters their Personal Identification Number (PIN) for verification on a payment device.

Chip-and-Signature: The method of processing a transaction in which the customer signs the sales draft rather than entering a PIN.

Chip Card: Also known as a smart card, a chip card features an embedded microchip that contains account data used to process payment transactions.

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

Code 10: A process by which a merchant contacts the telephone authorization center to alert for possible fraudulent card or transaction activity without alerting the cardholder.

Contactless Indicator: A symbol made up of five radiating arcs, indicating that a payment card or point-of-sale device is equipped with Near Field Communication (NFC) and can perform a contactless transaction.

Contactless Payment: A transaction carried out using a chip card or smart device, in which the customer waves or taps their card or device near an electronic payment device that captures card data for authorization.

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

Credit Card: A card that accesses a revolving credit account.

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

Cybercrime/Cyberattack: Any unlawful activity involving a computer system.

Cybersecurity: The protection of computer systems from hacking, identity theft, and malware intrusion.

Debit Card: A payment card that accesses a deposit account. Debit cards can be both signature-based and PIN-based at the point-of-sale.

Decline: A transaction response indicating the sale transaction is not approved or not authorized by the Card Issuing Bank.

Deposit Account: A personal or business checking or savings account at the merchant's Financial Institution that is used for funding card payment transactions and billing for processing services.

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/sales receipt as identified in the electronic record.

E-Commerce: An electronic commerce method of buying and selling goods and services online.

Embossed: Term that refers to the raised characters on the front of a payment card, including the cardholder's name, card account number, expiration date or valid dates. Many cards are no longer embossed but rather the cardholder information is printed on the card.

EMV: An acronym for Europay, Mastercard, and Visa. EMV refers to the increased security of payment card transactions using a chip embedded in credit, debit, and prepaid cards.

Encryption: A method for achieving data security by encoding messages or information in such a way that only authorized parties can access it.

Expiration Date: The date embossed or printed on a payment card to indicate the date after which the card is no longer valid (See also **Valid Dates**).

Factoring: See **Draft Laundering**.

Front-End Processing Platform: Responsible for obtaining the authorizations and sending sales transactions to the back-end processor/platform for settlement.

Gateway or Payment Gateway: Facilitates the routing of payment transactions from a merchant website's secure payments page (Shopping Cart) or point-of-sale software to the front-end processing platform for authorization/sale.

Hologram: A reflective image that appears on payment cards for enhanced security measures.

Identity Theft: A form of financial fraud in which a person assumes the identity of another person to obtain credit or for other financial gain.

Interchange Fees: Percentage rates on transaction and per transaction item fees set by the Card Associations.

IP or Internet Protocol: Communication through internet networks. An IP address is a unique set of numbers assigned to each internet connection or network device.

Key-Entered Transaction: A procedure performed by a merchant when the card chip or swipe reader is malfunctioning or if the card itself cannot be read or is not present. Instead of swiping or dipping the card, the merchant will manually enter the card information into the system.

Logos: Images of the Card Associations that appear on the card.

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

Malware: Malicious, harmful software that accesses a device without the user's knowledge. Types of malwares include spyware, phishing, viruses, and trojan horses.

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

Merchant Account: A processing account approved and setup by a Merchant Provider enabling the merchant to accept cards for payment.

Merchant Services Agreement: A contract between a merchant and a Merchant Provider that entitles the merchant to accept cards for payment.

Merchant ID Number: An identification number assigned to a Merchant Account by the Merchant Acquirer.

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

Mobile Acceptance: A payment solution that enables merchants to process credit and debit card transactions securely through a smart device and/or mobile reader.

Mobile Wallet: A smart device app in which consumers can store payment card credentials for the purpose of using the smart device as a payment device.

Mobile Payment/Mobile Commerce: A transaction that is conducted using a smart device as the payment device, rather than a payment card, check, or cash.

Near Field Communication (NFC): The technology that enables smart devices and other NFC payment devices to communicate and exchange data by bringing them in close proximity of one another.

Offline: An operating mode in which payment devices are not connected to a central computer. Responses are governed by guidelines set by the Card Issuing Bank. Can also be the use of a debit card without entering a PIN (referred to as a signature-based debit transaction).

Omnichannel: The concept of utilizing multiple communication channels to conduct business whether it be physical location, website, social media, live web chats, mobile applications, and/or telephone communication.

Online: An activity or service available on or performed using the internet or other computer network. 1) An operating mode in which payment devices are connected to a central computer, accessing the database for authorizations, and programming changes via a dial analog line, IP or WiFi connection or Cellular communication; 2) E-Commerce processing, where merchants allow customers to pay for goods or services "online" through electronic commerce; 3) Debit card processing using a PIN is referred to as an "online" debit transaction versus an "offline" signature-based debit transaction.

Partial Authorization: The means by which a merchant can process part of a transaction on a credit, debit, prepaid, or gift card, and then complete the rest of the transaction using a different payment method.

Payment Card: A financial transaction card issued by a Financial Institution.

Payment Card Industry Data Security Standard (PCI DSS): A globally accepted set of mandatory regulations and best practices for merchants and all entities that process payments that are designed to protect card data and reduce card fraud and identity theft.

Payment Device: A mechanism used by a merchant to authorize payment card information by reading it from the chip, the magnetic stripe on the card or through contactless means to obtain authorization.

Payment Networks: Mastercard, Visa, Discover, and American Express systems used for routing payment transactions from the point-of-sale through the Processor to the Card Issuing Bank. (See **Card Associations / Brands / Networks**.)

PCI DSS Compliance: Mandatory adherence to the regulations and best practices set forth in the PCI DSS. (See **Payment Card Industry Data Security Standard**)

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

Phishing: An attempt to gain information such as account numbers, usernames, passwords, and/or other account data through an email that appears to come from a trusted source.

PIN Debit Networks: Routes PIN-based debit transactions from the merchant to the Card Issuing Bank (cardholders' bank account). PIN Debit Networks are STAR, PULSE, MAESTRO, INTERLINK, etc.

PIN Pad/PIN Entry Device: An electronic device with a keypad or touch screen that customers use to enter their Personal Identification Number (PIN) to complete a transaction.

Point-of-Sale (POS): The merchant location from which a customer makes a purchase. May also be referencing the POS solution the merchant is using to process transactions.

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

Prepaid card: A payment card with a predetermined balance, such as a gift card.

Processing: Payment processing is a series of communication steps for settling electronic card payment transactions. Payments are initiated by a business accepting a card for payment through a payment device that sends the transaction to the front-end processor for authorization and capture and settled by the back-end host processor. Transactions are then routed from the back-end processor to the Card Issuing Bank for posting to the cardholder's billing statement and payment to the merchant.

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

Processor: Front-end processor/platform provides authorization and ticket capture and routes transactions to back-end processor. Back-end processor is where the Merchant Account resides. The back-end settles/funds merchant transactions and deposits and routes transactions through the Card Networks or Debit Networks (for PIN-based debit) to the Card Issuing Bank (cardholder statement). Back-end bills merchant for processing and provides month-end billing statement.

Radio Frequency Identification (RFID): A wireless system used to transmit payment information during the contactless payment process.

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

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

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 transaction receipt or paper form printed as the result of a payment.

Settlement: The process by which the amount of a payment card transaction is credited to a Merchant Account and debited to a cardholder's account.

Shopping Cart Abandonment: A practice by consumers of adding items to an online or mobile shopping cart and not completing the purchase.

Signature Panel: Found on the back of most payment cards where the cardholder signs the physical card.

Skimming: An electronic method of capturing card account data in order to commit financial fraud. A payment card is swiped through a small electronic device that records information from the card's magnetic stripe.

Smart Device: Mobile hardware with an advanced operating system that enables many of the functions of a computer, including payment processing via a mobile wallet and web access.

Split Sales Transaction: A prohibited practice of dividing the dollar amount of an individual sale either 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 or to avoid a declined response due to the card or transaction amount limit.

Split Tender Transaction: The practice of using two or more forms of payment (cash, check, credit, debit, prepaid, or gift card). Split tender transactions most often occur when consumers use gift cards to buy goods and services that cost more than the value of the card, or when two or more people want to split the check at a restaurant.

Supporting Documentation: The documents which provide proof or evidence necessary to contest a chargeback transaction.

Surcharge: An additional charge or fee added to the total amount of a card transaction to cover the merchant's cost of processing. The Card Associations as well as government entities have rules and regulations surrounding surcharge programs. Please contact your Merchant Provider if you would like more information on surcharging.

Tablet: A mobile device with functionality similar to a smartphone but usually larger in size.

Tap to Pay: The growing trend of tapping a payment card, smartphones, tablets, watches, etc. on or near a payment device to process a transaction using contactless capability.

Thermal Receipt Paper: A roll of paper where the surface is coated with a substance which changes color when heated above a certain temperature that is used by most payment devices to print transaction sale receipts/sales slips.

Tip Adjustment: Allows eligible merchant account types to adjust the authorized amount of a transaction prior to settlement but after an authorization has been obtained. The Merchant Account and payment device must be set up specifically to allow this function.

Transaction: Any action such as a purchase, refund, debit, etc. between a cardholder and a merchant.

Tokenization: A process by which the card account number is replaced with a substitute value called a "token" to keep the real account number safe and secure during an electronic transaction.

Unembossed Card: A payment card on which the name, account number, and valid dates are printed flat on the card's surface rather than being embossed onto the surface of the card.

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

Virtual Terminal: The means by which a merchant may process transactions via an online portal or website in lieu of a payment device. Transactions hand-keyed on a virtual terminal are deemed card-not-present.

WiFi: A connectivity method for a payment device using a wireless network protocol.

Zero Floor Limit: This term refers to a policy whereby merchants are required to obtain authorization for every transaction processed at their store, regardless of its size.