

IMPORTANT



INFORMATION

WHAT YOU NEED TO KNOW

U.S. merchants must follow basic card acceptance rules for all credit card transactions. Careful and consistent adherence to the USA rules outline in this section will help you to enhance customer satisfaction and increase your profitability. If you have any questions about any of the rules presented here, contact your merchant bank and failure to adhere to these could result in fines, termination of service, or both.

Acceptance Options:

Merchants accepting Visa, MasterCard, Discover, and AMEX must honor all cards presented to them by a cardholder.

Dollar Minimums & Maximums:

Imposing minimum or maximum purchase amounts is a violation of USA rules.

Surcharging:

You may not impose any surcharge to cardholders for using a credit card as a form of payment. You may, however, offer a discount for cash transactions, provided that the offer is clearly disclosed to customers and the cash price is presented as a discount from the standard price charged for all other forms of payment.

Convenience Fees:

For merchants who offer an alternate payment channel for customers to pay for goods or services, a convenience fee may be added to the transaction amount. The merchant **must** adhere to the following rules:

- The fee is being charged for a bona fide convenience of using an alternative payment channel outside of the merchant's normal business practice (see below).
- The Fee:
 - Must be disclosed to the customer as a charge for the convenience of using the alternate method to pay
 - Is applied only to non face-to-face transactions
 - Must be a flat or fixed amount, regardless of the amount of the payment due
 - Is applied to all forms of payment products accepted in the alternative payment channel
 - Is included as part of the total transaction amount
 - Cannot be added to a recurring transaction
 - Is assessed by the merchant that provides the goods or services to the cardholder and not a third party
- The customer must be given the opportunity to cancel prior to the completion of the transaction
 - **EXAMPLE:**
 - The merchant provides utility services to its customers, and the customary way to pay is by mail or in person at the merchant's location. For the convenience of its customers, the merchant also offers a website for payments. In this example, the merchant may apply a convenience fee to payments made via the website.

Taxes:

Include any required taxes in the total transaction amount. Do not collect taxes separately in cash.

Laundering:

Deposit transactions only for your own business. Depositing transaction for a business that does not have a valid merchant agreement is called laundering or factoring. Laundering is not allowed; it is a form of fraud associated with high chargeback rates and the potential for promoting illegal activity.

Zero-Percent Tip:

For restaurant, taxicabs, limousines, bars, taverns, beauty/barber shops, health/beauty spa merchant's transactions with a credit or debit card, authorize only for the known amount, not the transaction amount plus estimated tip. An authorization that includes an estimated tip can reduce a cardholder's available funds or credit by an unrecognizable or unexpected amount. This kind of transaction may occur if a cardholder leaves a cash tip or adds a tip that is less than the estimated amount used for authorization; for example, if a restaurant authorizes for an estimated 20 percent tip, but the customer adds on only 15 percent.

No Cash Refunds:

You are not permitted to issue cash refunds for any credit or debit card transaction. By issuing credits, you protect your customers from individuals who might fraudulently make a purchase on their account and then return the merchandise for cash. You may though give a cash refund for a transaction that was conducted with a prepaid card.

Deposit Time Limits:

Deposit your transactions within 5 calendar days of the transaction date. Depositing more than 30 days after the original transaction date may be charged back to you.

Delivery of Goods and Services:

Deliver the merchandise of services to the cardholder at the time of the transaction. Cardholders expect immediate delivery of goods and services unless delivery arrangements have been made.

Cardholder Information:

Keep cardholder account numbers and personal information confidential. Cardholders expect you to safeguard any personal or financial information they may give you in the course of a transaction.

AUTHORIZATION PROCESS

When swiping the card through the terminal, hold onto the card for the entire transaction process. If you cannot process the card by swiping it through the card reader, then look at one of the following to see if this is the problem:

- Damaged Magnetic Stripe Reader
- Dirty Magnetic Stripe Reader
- Improper Card Swiping
- Spilled Food or Drinks on the Terminal
- Magnetic Stripe Reader Obstruction (electrical units near the terminal)
- Anti Theft Devices near the Terminal

The authorization process allows the card Issuer to approve or decline a transaction. However, to prevent fraud the issuer may request additional information about the transaction.

Possible Codes:

- *Approved*
 - *Declined or Not Accepted*
 - *Call - Call Center or Referrals*
 - *Pick Up*
-

RETURNS & EXCHANGES

As a merchant you are responsible for establishing the merchandise returns and credit policies. Clear disclosure of these policies can help you avoid misunderstandings and potential cardholder disputes. Visa/MasterCard/Discover will support your policies, provided they are clearly disclosed to cardholders **BEFORE** the completion of a transaction.

Card-Present Transaction:

- **No Refunds or Returns.**
 - You are not willing to accept returned merchandise or merchandise exchanges.
- **Exchange Only:**
 - You are willing to exchange returned merchandise for similar merchandise that is equal in price to the amount of the original transaction.
- **In-Store Credit Only:**
 - You are willing to take returned merchandise and give the cardholder an in-store credit for the value of the merchandise.
- **Special Circumstances:**
 - You and the cardholder have agreed on some special terms and that agreement is written on the customer receipt or related document. The cardholder's signature on the receipt or related document indicates acceptance of the agreed-upon terms.

Mail Order or Telephone Order

For proper disclosure, your refund and credit policies must be mailed, e-mailed, or faxed to the cardholder. To complete the sale, the cardholder must sign and return the disclosure statement to you.

CARD-NOT-PRESENT PROCEDURES

The following outlines basic fraud prevention guidelines and best practices for card-not present transactions.

- **You must take a manual imprint of all cards not swiped through the terminal and have the customer sign the imprinted sheet!**
- Authorization is required on ALL card-not-present procedures and should occur before any merchandise is shipped or service performed.
- Ask for the expiration date and include it in the authorization call.
- Ask for the CVV2 number. This is the last three digits, located in the signature panel on the back of the card. This must be provided in the authorization process. This will reduce your fraud-related charge-backs.
 - If there is no CVV2 number you will be asked to respond to the following:
 1. 0 = CVV2 is not included in the authorization.
 2. 1 = CVV2 is included in the authorization.
 3. 2 = Cardholder has stated that CVV2 is illegible.
 4. 9 = Cardholder has stated that CVV2 number is not on the card.
 - Here are the results you will see for CVV2
 1. M = Match and ok to complete the transaction.
 2. N = No match: Potential Fraud
 3. P = CVV2 request not processed. Resubmit the information
 4. S = CVV2 follow up with the customer to insure that the CVV2 is not present.
 5. U = Evaluate all available information and decide whether to proceed.

AVS

You may ask your client for their address as it appears on their monthly billing statement. You would simply be required to enter ONLY THE NUMERICAL portion of the address, and the zip code. (9 digits if possible) Your response will be one of the following:

- Y = Match. Both the Street Address and five digit Zip Code matched and you can be confident that the transaction is legitimate.
- A = Partial Match. Street Address matches but Zip Code does not. Potential Fraud and it's your decision on whether to continue the transaction or not.
- Z = Partial Match. Zip Code matches but Street Address does not. Potential Fraud and it's your choice to continue the transaction or not.
- N = No Match. Neither the Street Address nor Zip Code matches. Look for other information for validation regarding the card.
- U = Unavailable. No support from the issuer of the card and it's your decision to Continue the transaction or not.
- R = Retry. Issuers system is busy or not available. Try again later or it's your decision to continue.

SUSPICIOUS TRANSACTIONS

These tips are provided to help you design policies and procedures for your staff in combating fraud.

Watch Out for Customers Who:

- Purchase a lot of merchandise without regard to size, style, color, or price.
- Ask no questions on major purchases.
- Try to distract or rush you during the sale.
- Make purchases, leave the store, and return to make more purchases.
- Make large purchases right at the opening or at the last minute when the store is closing.
- Refuse free delivery for large items.
- Orders shipped to an International address.
- Hesitation when customer is providing personal information.
- Orders from Internet addresses at free e-mail services.
- Orders on multiple cards but shipped to the same address.
- Multiple shipping addresses.
- Multiple cards from a single IP address.

If you have any concerns about any of these signs, please make a call to the voice authorization center and say, "I have a Code 10 authorization request." (See Code 10 Calls)

Skimming

Skimming is a fraud scam in which a cardholder's account information is electronically copied, or "skimmed" off the card's magnetic stripe, often in the process of an otherwise valid transaction. The skimmed information is used to produce counterfeit payment cards that are, in turn, used for fraudulent transactions.

Skimming often occurs in card-present environments, such as restaurants and service stations, where transaction processing may occur out of sight of the cardholder. To skim a card, fraudsters typically use a small portable device that may not be bigger than a pager. They swipe the card through the device to copy the magnetic stripe.

To prevent skimming, you should be on the lookout for:

- Anyone operating an electronic device not normally used in your day-to-day business activities.
- Anyone offering you money to record account information.

If you suspect skimming activity at your place of business, you should call your merchant back or company security **immediately**.

CODE 10 CALLS

Code 10 calls allow merchants to alert card issuers to suspicious activity and take appropriate action when instructed to do so. You should make a Code 10 call to your voice authorization center whenever you are suspicious about a card, cardholder, or a transaction. The term “Code 10” is used so the call can be made at any time during a transaction without arousing a customer’s suspicions.

To Make a Code 10 call:

- Keep the card in your possession during the call.
- Call your voice authorization center, and say, “I have a Code 10 authorization request.”
 - The call may first be routed to a representative at your merchant bank who may need to ask you for some merchant or transaction details. You will then be transferred to the card issuer and connected to a special operator who will ask you a series of questions that can be answered with a simple yes or no.
- When connected to the special operator, answer all questions calmly and in a normal tone or voice. Your answers will be used to determine whether the card is valid.
- Follow all operator instructions.
- If the operator tells you to pick up the card, do so only if recovery is possible by reasonable and peaceful means.

Making Code 10 Calls after a Transaction:

Sometimes a sales associate may not feel comfortable making a Code 10 call while the cardholder is at the point of sale, or the sales associate may become suspicious of a cardholder who has already left the store. Emphasize to your sales staff that they can make Code 10 calls even after a cardholder leaves the store. A Code 10 alert at this time may help stop fraudulent card use at another location, or perhaps during a future transaction at your store.

CHARGEBACKS

A chargeback is a transaction that a credit card Issuer returns to a merchant bank as a financial liability and which, in turn, a merchant bank may return to a merchant. In essence, it reverses a sales transaction, as follows:

- The card issuer subtracts the transaction dollar amount from the cardholder’s account. The cardholder receives a credit and is no longer financially responsible for the dollar amount of the transaction.
- The card issuer debits the merchant bank for the dollar amount of the transaction.
- The merchant bank will, most often, deduct the transaction dollar amount from the merchant’s account. The merchant loses the dollar amount of the transaction.

For merchants, chargebacks can be costly. You can lose both the dollar amount of the transaction being charged back and the related merchandise. You also incur your own internal costs for processing the chargeback and be assessed a fee from the processor.

Why Chargebacks Occur:

The most common reasons for chargebacks include:

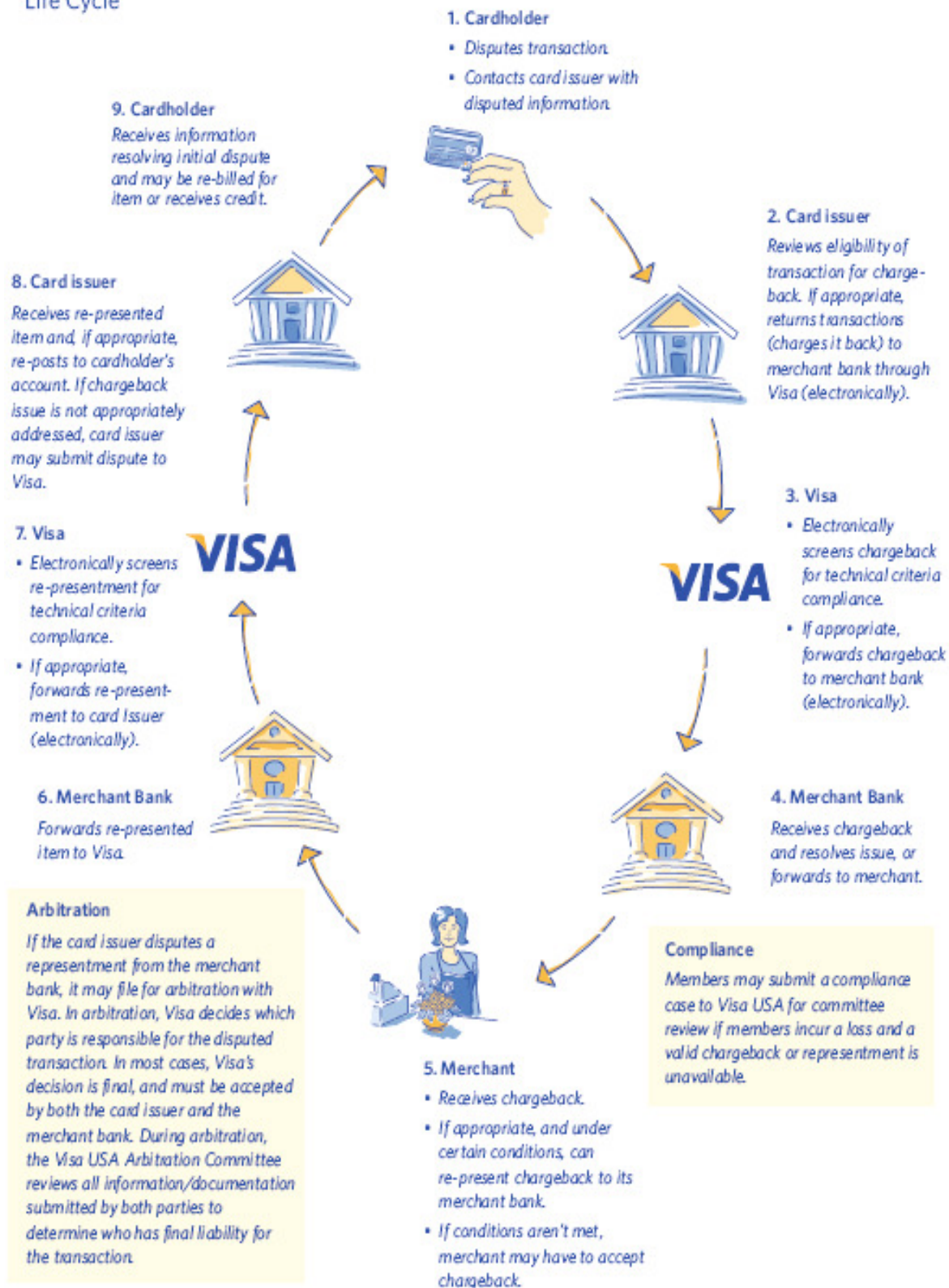
- Customer Disputes
 - A credit has not been processed as promised.
 - Merchandise ordered was never received.
 - A service was not performed as expected.
 - The customer did not make the purchase; it was fraudulent.
- Fraud
- Processing Errors
- Authorization Issues
- Nonfulfillment of Copy Requests (only if fraud or illegible)

Although you probably cannot avoid chargebacks completely, you can take steps to reduce or prevent them. Many chargebacks result from easily avoidable mistakes, so the more you know about proper transaction-processing procedures, the less likely you will be to inadvertently do, or fail to do, something that might result in a chargeback (see *Avoiding Chargebacks*).

Of course, chargebacks are not always the result of something merchants did or did not do. Errors are also made by merchant banks, card issuers, and cardholders.

The Chargeback Life Cycle

The following illustration shows the chargeback life cycle.



AVOIDING CHARGEBACKS

Most chargeback's can be attributed to improper transaction-processing procedures and can be prevented with appropriate training and attention to detail. The following best practices will help you minimize chargebacks.

- **Declined Authorizations**
 - If the card was declined once, ask for another form of payment.
 - **Transaction Amount**
 - Do not estimate transaction amount totals. Be exact!
 - **Referrals**
 - If you receive a "Call" message in response to an authorization request, do not accept the transaction until you have called your authorization center.
 - **Expired Card**
 - Do not accept a card after its "Good Thru" or "Valid Thru" date.
 - **Card Imprint for Key-Entered, Card Present Transaction**
 - If, for any reason, you must key-enter a transaction to complete a card-present sale, make an imprint of the front of the card on the sales receipt, using a manual imprinter.
 - **Cardholder Signature**
 - The cardholder's signature is required for all card-present transactions. Failure to obtain the cardholder's signature could result in a chargeback if the card holder later denies authorizing or participating in the transaction.
 - **Digitized Cardholder Signature**
 - You must always compare the customer's signature on the sales receipt with the hand-written signature in the signature panel and digital signature on the front of the card. Do not always go by the digital signature.
 - **Fraudulent Card-Present Transaction**
 - If the cardholder is present and has the account number but not the card, do not accept the transaction. NO CARD, NO TRANSACTION!
 - **Legibility**
 - Ensure that the transaction information on the sales receipt is complete, accurate, and legible before completing the sale.
 - **Voiding Incorrect or Duplicate Sales Receipts**
 - Ensure that incorrect or duplicate sales receipts are voided and that transactions are processed only once.
 - **Disclosing Refund, Return, or Service Cancellation Policies**
 - All policies must be disclosed in the cardholder at the time of the transaction. Policies should be pre-printed on your sales receipts or clearly displayed.
 - **Record Keeping**
 - Keep all sales receipts for a minimum of six months from the delivery of your product or service. Those will coincide with the customer's timeframe to file a request for a cancellation of the sale.
- Again, make sure that your refund policy is clearly stated on your receipt. If you receive a notice of a pending chargeback, you should call us immediately so that we can help you with the process. Typically, you are given a very rigid timeline to respond to the request for information. Let schmooze help you with this to avoid unnecessary expense and frustration.

RECOVERED CARDS

In general, you should recover a card if you have reasonable grounds for believing the card is being used fraudulently or is altered or counterfeit. The following situations are considered reasonable grounds for recovery:




- Card security features are missing or irregular, or appear to have been tampered with.
- The account number on the magnetic stripe does not match the number embossed on the front of the card.
- You receive a pick-up response when a card has been swiped for electronic authorization, or you are instructed to recover the card during a **CODE 10 CALL** (see CODE 10 call section).

Card Recovery Procedures:

- Recover the card only if you can do safely. **Never take unnecessary risks.**
- Tell the cardholder you have been instructed to keep the card, and that he or she may need to call their issuer for more information.
- Remain calm and courteous. If the customer behaves belligerently, return the card immediately.
- Following a successful recovery, call your merchant bank and ask for further instructions.
- Cut the card in half lengthwise, being careful not to damage the dove hologram, the embossed account number, or magnetic stripe.
- Send the card pieces directly to your merchant bank.

Cash Rewards:

Cash rewards are available to merchants and their employees for recovering counterfeit or other fraudulent cards, or for information leading to the arrest and conviction of any person or persons involved in a counterfeit scheme. Eligibility for specific rewards is as follows:

-  \$50.00: A recovery after a pick-up response to an authorization request.
-  \$100.00: A recovery as a result of a **CODE 10 CALL**, you initiated.
-  \$1000.00: Leading to the arrest and conviction of any person using or causing a counterfeit card to be used.

To be eligible for the reward, you must comply with all card recovery rules. If a law enforcement agency keeps the recovered card, you must provide a legible copy of the front and back of the card back to the processing company.

WEB SITE INFORMATION

The following represents the minimum information that is recommended/required to be displayed on your website. These elements are intended to promote ease of use for online shoppers and reduce cardholder disputes and potential charge-backs.

- **Complete Description of Goods and Services**
 - Because of your “global market”, there is potential for misunderstandings. Provide as much information as possible.
- **Customer Service Information**
 - Include your phone number(s) and email address(es)
- **Return, Refund and Cancellation Policy**
 - This must be clearly posted.
- **Delivery Policy**
 - You set your own policies. Any restrictions on delivery must be clearly stated.
- **Country of Origin**
 - You must disclose the permanent address of your company.

Suggested “Best Practices”

- **Privacy Statement**
 - Security controls that you employ to protect your customers
- **Information on when Credit Cards are Charged**
 - You should not bill the customer until merchandise has been shipped
- **Order-fulfillment Information**
 - State timeframes for order processing, order confirmation, and order summary within one business day of original order
- **Customer Service Timeframes**
 - Ideally customer service e-mails or phone calls should be answered within two business days.
- **A Statement on Web Site regarding Security Controls used to Protect Customers.**
- **A Statement encouraging Cardholders to Retain a Copy of the Transaction.**