Understanding Chargebacks

PART TWO

Training & Tips To Reduce Risk

Bankers Insurance Group
Global Institutional Solutions

Table of Contents

Understanding Chargebacks: Training & Tips to Reduce Risk

Importance of Staff Training 3

Transaction Processing 4-5

Point of Sale 4

Transaction Settlement 5

Service Issues 5

Retrieval Requests 5

Retrieval Requests 6

Card-Present Environments 7

Authorizing Transactions 7

Credit Cards that Do Not Swipe 7

POS Electronic Systems 7

Unembossed Cards 8

Code '10' Procedures 8

Card-Not-Present Environments 9

CNP Prevention Tools 9-10

Payer Authentication 9

Shipping Physical Product 9

Address Verification Service 10

Card Validation 10

Verified by VISA 10

Most Common Chargeback Codes 11-13

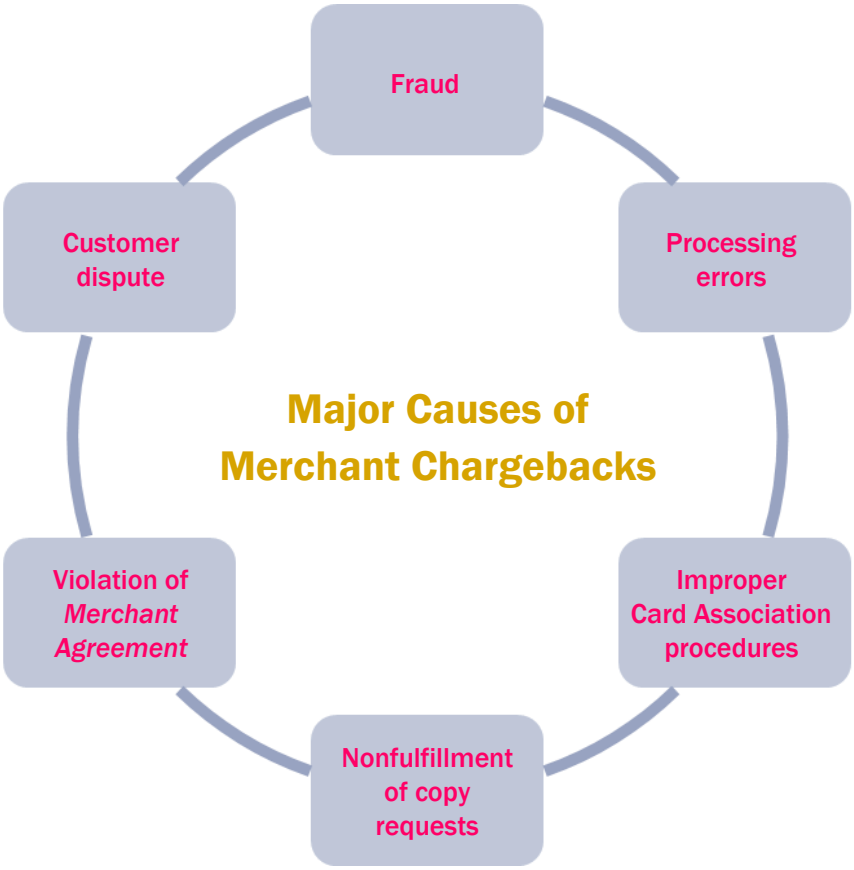
VISA 11-12

MasterCard 12-13

Importance of Staff Training

Staff training is one of the most effective proactive measures for reducing the incidence of chargebacks.

Some chargebacks result from avoidable mistakes. Consequently, the more informed and knowledgeable your staff is regarding the most appropriate transaction-processing procedures, they will become less likely to process transactions that could result in a chargeback. Remember, chargebacks can be costly: you can lose the dollar amount of the transaction, the related merchandise, and any costs associated with processing the chargeback.



Providing your staff with appropriate training with respect to card acceptance policies and procedures will:

- Give these folks the skills and knowledge to assist them to do their jobs more accurately and confidently.
- Enhance their level of customer service.
- Reduce your company's exposure to fraudulent transactions.
- Reduce other operating losses by decreasing the incidence of retrieval requests.

Transaction Processing

Chargebacks can result from improper transaction processing and may be reduced with proper training and attention.

Point of Sale

Card Validity

Ensure that the card being presented is valid and that standard identification and security features have been verified.

Card Imprint

If you are using a manual imprinter, confirm that the card number, expiration date, and customer signature are clearly visible on all copies of the sales slip. In addition, record the authorization number on the sales slip.

Cardholder Signature

The cardholder's signature is required for all card-present transactions, with the exception of unattended terminals and merchants participating in MasterCard's QPS (Quick Payment Service) or Visa's NSR (No Signature Required) program. Failure to obtain a signature could result in a chargeback if the cardholder denies authorizing the transaction. Verify the customer's signature to what appears on the card.

Declined Authorization

If the authorization request returns a declined response, do not complete the transaction and do not repeat the authorization request. Ask the customer for another form of payment.

Referrals

If your authorization request results in a "Call" message, call your authorization center prior to finalizing the transaction.

Expired Card

Do not accept a card after its expiry date unless an authorization approval for the transaction has been obtained from the card issuer.

Card Not Present

If the cardholder is present and has the card number but not the card, decline the transaction. Even with an authorization, the transaction may be fraudulent and charged back to you.

Legibility

Before completing a sale, ensure that the transaction information on the sales receipt is complete, precise and legible. Illegible receipts produce illegible copies and as a result, cannot be processed accurately.

Transaction Processing (Continued)

Transaction Settlement

Duplicating Transactions

There should be one entry for each transaction. Ensure that each transaction has been entered and deposited only once.

Incorrect/Duplicate Sales Receipt

Void incorrect or duplicate sales receipts immediately.

Billing Cardholders

Attempt to settle transactions as soon as possible; do not hold on to or delay them, as per the terms and conditions of your merchant agreement.

Recurring Transactions

Maintain a record of recurring payment transactions. If a cardholder cancels/changes a recurring payment arrangement, ensure that your records are updated to reflect this. If a transaction is submitted after a customer cancels/changes a recurring payment arrangement, a chargeback may result.

Service Issues

Stock & Delivery

Advise the customer if the merchandise purchased is out of stock or will be delayed in delivery. This will help to avoid unnecessary cancellations and chargebacks.

Refund/Exchange Policies

The terms and conditions of your merchant agreement require that you disclose to the customer the refund, exchange, or service cancellation policies your business has, especially on the sales receipt signed by the customer. This will help to avoid any cardholder disputes and/or misunderstandings.

Retrieval Requests

Retrieval Timeframes

Provide prompt responses to retrieval requests within the required timeframes in an attempt to avoid documentation related chargebacks.

Duplicate Requests

Respond to all retrieval requests, even if they appear to be duplicates.

Retrieval Requests

You may be requested to provide legible copies of sales drafts or transaction records for issuing financial institutions that need clarification on charges made to cardholder accounts or for possible fraud and/or other disputes. You are required to retain sales receipts for a minimum of 18 months from the transaction date.

The following documents may be used to bill transactions to cardholder accounts:

- Manual sales slips
- POS terminal transaction receipts
- Invoices
- Hotel guest folios
- Purchase order forms
- Car rental contracts
- Airline tickets

Responses to retrieval requests must be faxed/sent according to the instructions and timeframe indicated in the retrieval request letter. Your response to requests must be legible and include the following elements:

- Card number
- Cardholder name
- Cardholder signature (if applicable)
- Merchant name
- Merchant location
- Transaction date
- Transaction amount
- Expiry date
- Or any other document as requested

Failure to respond to a retrieval request will automatically cause you to lose a chargeback dispute.

Respond to all retrieval requests, even if they appear to be duplicates.

Additional Suggestions

Cardholders must be able to look at their statements and recognize transactions that occurred at your establishment.

Train sales staff

- Follow proper card acceptance procedures
- Review transaction receipts for accuracy and clarity
- Retain the original signed copy of the sales receipt

Avoid illegible transaction receipts

- Routine point-of-sale (POS) printer cartridge maintenance
- Changing POS printer paper when the colored streak first appears
- Retaining the original signed copy of the transaction receipt for better photocopying quality
- Handle carbon-backed, silver-backed and carbonless paper carefully.

Card-Present Environments

Authorizing Transactions

- When authorizing a transaction, ensure that the card is swiped in the direction indicated on the terminal.
- Authorize the amount and verify the authorization response.
- Verify the signatures. If the signatures do not match, request additional identification. If they still don't match, request a Code 10 authorization.
- If the embossed name and numbers do not match those printed on the receipt, request a Code 10 authorization.
- If the signature panel is blank, review valid identification such as a driver's license. Ensure the customer signs the card promptly and decline the transaction if the cardholder refuses.

Credit Cards That Do Not Swipe

When the magnetic stripe cannot be read, a manual imprint must be taken. Failure to do this may result in financial loss to your company.

Manual sales draft must include:

- The date
- An imprint of the credit card
- Details of the transaction
- Dollar amount
- Customer signature
- Authorization Number/Code

Note: Do not write "VOID" or "COPY" on the draft. Manually key in the card number to obtain authorization

On the POS terminal receipt:

- Print "PROOF COPY" on the signature line
- Write the pre-printed reference number as it appears on the manual sales draft
- Retain copies of both the manual sales draft and the POS transaction receipt needed to fulfill any retrieval requests.

POS Electronic System Is Unavailable Or Not Responding

- Take a manual imprint of the card.
- Phone for authorization and record the authorization number on the manual sales draft.
- Have the customer sign the imprinted copy.
- When the system is restored, Force Post the transaction on your POS device using the assigned authorization number.

Unembossed Cards

Unembossed Cards are similar to the cards you currently accept. They may take the form of a credit, debit, or prepaid/gift card, and will have the same familiar brand mark such as VISA and MasterCard. There is, however, one major difference – the card will look "flat". All account information – cardholder name, primary account number (PAN), validity date, and security character – is projected onto the front of the card with tamper-evident laser engraving or indent printing rather than embossing.

"Electronic Use Only" must be printed on the front of the card.

Unembossed cards can only be used in electronic terminals that are capable of online authorization. They cannot be keyed in. If a POS terminal is not available, merchants may follow the existing procedure for off-line authorization, however, the merchant is at greater risk of receiving a "Missing Imprint" or "Card Not Present" dispute/chargeback.

Code '10' Procedures

Code '10' calls allow merchants to alert card issuers to suspicious cards, cardholders or transactions.

Common characteristics of suspicious activity:

- The card has been altered.
- The card number on the card does not match the card displayed on the receipt.
- The customer's behavior leads you to believe that something is "wrong".
- Signature does not match the signature on the back of the card.

To Make a Code "10" call:

- Keep the card in your possession during the call.
- Call your voice authorization center and request a "Code 10" authorization.
- The operator will ask a series of questions to determine the validity of the card.
- If you are requested to retain the card, attempt to do so by peaceful and reasonable means.

Card-Not-Present Environments

If you are able to process remote transactions under your merchant agreement, it is recommended that you refer to and review the terms and conditions related to these types of transactions.

The following prevention indicators and tools may assist you in reducing the risk of fraud-related chargebacks and losses. In addition, card-not-present merchants should develop fraud control policies and training for employees. Recognize potential indicators of fraud such as:

Online and mail order merchants are the most vulnerable to chargebacks from "friendly fraud."

- First-time shoppers
- Larger-than-normal orders
- Orders that include multiples of the same item
- "Big-ticket" item purchases
- "Rush" or "overnight" shipping
- Shipping to international addresses
- Transactions with similar account numbers
- Shipping to a single address, but transactions placed on multiple cards
- Multiple transactions on one card over a short period of time
- Multiple transactions on one card with a single billing address but multiple shipping addresses
- Online transactions: multiple cards used from a single IP address
- Orders from addresses of free e-mail services

Card-Not-Present Prevention Tools

Payer Authentication

In the ecommerce environment, Payer Authentication programs, like Verified by Visa and MasterCard SecureCode can help merchants to reduce chargebacks and losses due to friendly fraud. Participating in these programs can create a chargeback liability shift from the merchant and the acquiring bank to the cardholder's issuing bank. The cardholder can still commit friendly fraud, but it is no longer the merchant's problem: the issuing bank is responsible for the chargeback.

Shipping Physical Product

Physical product should only be shipped to the billing address of the credit card. Use a delivery service or courier that requires signature on delivery and provides order tracking and delivery confirmation. Always require the signature of the cardholder only upon delivery. Getting the cardholder's signature on delivery at the billing address of the credit card can reduce the cardholder's ability to dispute on a claim of an unauthorized transaction.

Card-Not-Present Prevention Tools (Continued)

AVS – Address Verification Service

- AVS provides merchants with a method to verify the billing address given by the cardholder, to the billing address on file with the credit card issuing bank.
- Participating cards: Visa, MasterCard and Discover®, all with similar features.
- It is important to note that AVS is only a tool and is most effective when used in conjunction with other fraud tools and risk indicators.
- Regardless of the AVS result, if the card Issuer does not approve the authorization request, do not complete the transaction.

CVD – Card Validation Digit (CVV2, CVC2, CID)

- CVD is a 3 digit code printed in the signature panel of Visa, MasterCard and American Express® issued cards and 4 digit code printed on the front of American Express® cards.
- This code helps to ensure that the customer making the Mail Order/Telephone Order or eCommerce transaction is in possession of his or her credit card.
- Be vigilant if the customer cannot provide the CVD code or the code does not match to that on file with the Issuer, it's more than likely that the card is not present and the number given could be stolen. In the case of an unmatched code, ask the customer to confirm it and if it still does not match, further validate or decline the transaction.
- Regardless of the 3 or 4 digit code verification response, if the card Issuer does not approve the authorization request, do not complete the transaction.

VBV – Verified By Visa

- Most effective with online business types as it offers protection against fraud-related chargebacks. It allows customers to verify their identity at the time of purchase through the use of his or her personal password.
- Can help to reduce fraudulent transactions and fraud-related chargebacks.
- Increased cardholder confidence may lead to increased sales.

Most Common Chargeback Codes

VISA

AUTHORIZATION RELATED

RC44 *Transaction exceeds floor limit and not authorized/Declined authorization*

Suggestions to avoid this issue

- Authorize all transactions above your established floor limit on the transaction date and record the authorization code on the transaction receipt.
- Do not process a transaction if the authorization request received a decline response. Return the card to the customer and request payment by another means.

Special Remedy Instructions

- Provide proof of a valid authorization number at the time of the transaction.

DOCUMENTATION RELATED

RC45 *Copy not received within the required timeframe*

Suggestions to avoid this issue

- Retain all sales slips for the time specified as per merchant agreement (18 months).
- Respond to all retrieval requests promptly by supplying copies of requested sales slips and related documentation. Failure to supply a copy of the requested transaction information within the specified timeframe could result in a non-reversible chargeback debit being processed to your account.
- Ensure all sales slips are complete, clear and legible whether manually imprinted or electronically through a terminal printer.
- Ensure that the correct sales receipts are supplied for the reference numbers provided in each retrieval request.

FRAUD RELATED

RC35 *Missing signature*
RC39 *Missing imprint*
RC41 *Non-possession of card*
RC49 *Other – Cardholder did not authorized/participate*

Suggestions to avoid these issues

- For all face-to-face transactions, it is imperative that an Electronic or Manual Imprint and Signature appears on the transaction receipt.
- All retrieval requests must be fulfilled within the required timeframe.
- Do not alter a cardholder's transaction receipt or other documentation after the sale is completed.
- If you choose to accept a mail order/telephone order or non-secure Electronic Commerce, ensure you record the Cardholder's name, address, phone number, and e-mail address. After the order is completed, call the cardholder to confirm the information given or verify with the card Issuer the information the cardholder provided. If approved by either the card holder or card Issuer, retain proof of approval and who you spoke with.

Most Common Chargeback Codes (Continued)

VISA

PROCESSING ERRORS

RC33 *Duplicate processing*

Suggestions to avoid this issue

- Ensure all transactions are deposited within the required timeframe (3 business days).
- Ensure all cards accepted are Visa cards with the Visa Logo and security features.
- Avoid duplicating a purchase by billing the cardholder more than once. If you realize an error of duplication, promptly issue a credit to the cardholder's account.
- Ensure all refunds are posted as refunds and not refund corrections.
- Transaction amounts must be legible on all copies of the transaction receipt.

Special Remedy Instructions

- Card-Present Environment – Two swiped/imprinted and signed sales drafts.
- Card-Not-Present Environment – Two authorized separate transactions.

NON-RECEIPT OF MERCHANDISE OR SERVICES

RC38 *Merchandise/services not received by cardholder or authorized person*

Suggestions to avoid this issue

- Ensure merchandise/service is received by the Visa cardholder or authorized person on the agreed upon delivery date and the agreed upon location (retain signed delivery receipt showing name and address merchandise was delivered to).

Special Remedy Instructions

- Obtain signed proof of delivery by cardholder at the agreed upon location.

MasterCard

AUTHORIZATION RELATED

RC08 *Requested/Required authorization not received*

Suggestions to avoid this issue

- Always obtain proper authorization for all transactions being processed.
- Do not process transactions for more than the authorized or pre-authorized amount.
- If dollar value of transaction exceeds the pre-authorization amount merchant is to obtain additional authorization for the difference or re-authorize the entire amount of transaction.
- Avoid processing transactions for which "declined" authorization responses are received.

Most Common Chargeback Codes (Continued)

MasterCard

DOCUMENTATION RELATED

RC01 *Requested transaction information not received*

Suggestions to avoid this issue

- Retain all sales slips for the time specified as per merchant agreement (18 months).
- Respond to all retrieval requests promptly by supplying copies of requested sales slips and related documentation. Failure to supply a copy of the requested transaction information within the specified timeframe could result in a non-reversible chargeback debit being processed to your account.
- Ensure all sales slips are complete, clear and legible whether manually imprinted or electronically through a terminal printer.
- Ensure that the correct sales receipts are supplied for the reference numbers provided in each retrieval request.

FRAUD RELATED

RC37 *No cardholder authorization*

Suggestions to avoid this issue

- Ensure that all face-to-face transactions are completed with a card swipe via a POS terminal or with a manual imprint including a cardholder signature, the amount and an authorization number.

Special Remedy Instructions

- Provide a copy of the signed swiped/imprinted and authorized sales slip.
- An authorization log from the POS terminal must be provided in addition to the copy of the transaction slip.

FRAUD RELATED

RC40 *Fraudulent processing of transactions*

Suggestions to avoid this issue

- Ensure the cardholder is contacted and agrees to any additional charges to their credit card via a signed swiped/imprinted and authorized sales slip.

Special Remedy Instructions

- Provide a copy of both the disputed and non-disputed transaction as well as a description of the purchase or service that was provided for each transaction.