



Chargeback Management Guidelines for Visa Merchants



Table of Contents

Introduction	1
Section 1: Getting Down to Basics	5
Visa Transaction Processing—Who is Involved?	6
Visa Transaction Flow for Magnetic-Stripe and Chip Cards	7
Visa Transaction Flow for PIN-Based Point-of-Sale and ATM	9
Cardholder Disputes and Chargebacks	11
Visa Rules	13
Visa Rules for Returns and Exchanges	18
Section 2: Copy Requests	21
Transaction Receipt Requirements—Card-Present Merchants	22
Transaction Receipt Requirements—Card-Absent Merchants	23
Responding to Copy Requests	24
How to Minimize Copy Requests	26
Section 3: Chargebacks	29
Why Chargebacks Occur	30
Customer Dispute Chargebacks	31
Invalid Chargebacks	32
Minimizing Chargebacks	33
Chargeback Monitoring	38
When Chargeback Rights Do Not Apply	40
Section 4: Chargeback Reason Codes	41
Reason Code 30: Services Not Provided or Merchandise Not Received	43
Reason Code 41: Cancelled Recurring Transaction	46
Reason Code 53: Not as Described or Defective Merchandise	49
Reason Code 57: Fraudulent Multiple Transactions	52
Reason Code 60: Illegible Fulfillment	53
Reason Code 62: Counterfeit Transaction	55
Reason Code 71: Declined Authorization	57
Reason Code 72: No Authorization	59
Reason Code 73: Expired Card	62
Reason Code 74: Late Presentment	64

Table of Contents

Reason Code 75: Transaction Not Recognized	66
Reason Code 76: Incorrect Currency or Transaction Code or Domestic Transaction Processing Violation.	67
Reason Code 77: Non-Matching Account Number	69
Reason Code 80: Incorrect Transaction Amount or Account Number	72
Reason Code 81: Fraud—Card-Present Environment	74
Reason Code 82: Duplicate Processing	78
Reason Code 83: Fraud—Card-Absent Environment	80
Reason Code 85: Credit Not Processed	83
Reason Code 86: Paid by Other Means	88
Reason Code 96: Transaction Exceeds Limited Amount	89
Appendix 1: Training Your Staff	91
Appendix 2: Glossary	93
Appendix 3: Visa Europe Territory	101

Introduction

Purpose

The Chargeback Management Guidelines for Visa Merchants is a comprehensive manual for all businesses that accept Visa transactions. The purpose of this guide is to provide merchants and their back-office sales staff with accurate, up-to-date information to help merchants minimizing the risk of loss from fraud and chargebacks. This document covers chargeback requirements and best practices for processing transactions that are charged back to the merchant by their acquirer.

Audience

This book is targeted at both card-present and card-absent merchants and their employees outside of the jurisdiction of Visa Europe, which may have different practices and requirements.

Contents

The Chargeback Management Guidelines for Visa Merchants contains detailed information on the most common types of chargebacks merchants receive and what can be done to remedy or prevent them. It is organized to help users find the information they need quickly and easily. The table of contents serves as an index of the topics and material covered.

Topics covered include:

- ✓ **Section 1: Getting Down to Basics**—Provides an overview of how Visa transactions are processed, from point of transaction to clearing and settlement. A list of key Visa policies for merchants is also included.
- ✓ **Section 2: Copy Requests**—Includes requirements and best practices for responding to a request for a copy of a sales receipt to resolve a cardholder dispute. Information on minimizing copy requests, ensuring legible receipts, and meeting sales draft requirements are also covered.
- ✓ **Section 3: Chargebacks**—Highlights strategies for chargeback prevention, as well as information on how and when to resubmit a charged-back transaction to your acquirer. A brief compliance process overview is also included.
- ✓ **Section 4: Chargeback Reason Codes**—Contains detailed information on the reason codes for the most common types of chargebacks that merchants receive. For each reason code, a definition, is provided along with the merchant's actions—or failure to act—that may have caused the chargeback, and recommendations are given for resubmitting the transaction and preventing similar chargebacks in the future.
- ✓ **Appendix 1: Training Your Staff**—A reference to Visa.com which offers resources that merchants can use for training their employees on card acceptance and fraud prevention procedures.
- ✓ **Appendix 2: Glossary**—A list of terms used in the guide.
- ✓ **Appendix 3: Visa Europe Territory**—A list of Visa European Territories.

Important
Note About
Country
Differences

Most of the information and best practices contained in the *Chargeback Management Guidelines for Visa Merchants* pertain to all regions; however in some countries, there are specific products, services, and regulatory differences that must be noted. In these instances, country or region-specific details have been identified with a universally recognized icon for the country or region under discussion.

It is important to note that the Visa payment system is operated in European economic area by Visa Europe, a separate company operating under license from Visa Inc.

Participation in the Visa payment system in such countries is governed by the *Visa Europe Operating Regulations*, rather than the *Visa International Operating Regulations*. While the *Visa Europe Operating Regulations* share many core requirements to ensure interoperability, such rules and best practices may vary from the guidelines set forth in this document. Please see Appendix 3 for a list of countries within Visa Europe.



United States



Canada



Latin America and Caribbean (LAC)



Asia Pacific (AP)



Central Europe, Middle East, and Africa (CEMEA)

Guide
Navigation

The *Chargeback Management Guidelines for Visa Merchants* provides icons that highlight additional resources or information:

Icon:



Definition:

Additional insights related to the topic that is being covered.



A brief explanation of additional Visa resources that are pertinent to the topic at hand.

Disclaimer

The information in this guide is current as of the date of printing. However, card chargeback procedures are subject to change. This guide contains information based on the current *Visa International Operating Regulations*. If there are any differences between the *Visa International Operating Regulations* and this guide, the *Visa International Operating Regulations* will prevail in every instance. Your merchant agreement and the *Visa International Operating Regulations* take precedence over this guide or any updates to its information. To access a copy of the *Visa International Operating Regulations*, visit www.visa.com/merchant, and click on Operations and Procedures.

All rules discussed in this guide may not apply to all countries. Local laws and rules may exist and it is your responsibility to ensure your business complies with all applicable laws and regulations.

The information, recommendations or “best practices” contained in this guide are provided “AS IS” and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice.

This guide does not provide legal advice, analysis or opinion. Your institution should consult its own legal counsel to ensure that any action taken based on the information in this guide is in full compliance with all applicable laws, regulations and other legal requirements.

Visa is not responsible for your use of the information contained in this guide (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party’s intellectual property rights, any warranty that the information will meet your requirements, or any warranty that the information is updated and will be error free.

For further information about the rules or practices covered in this guide, contact your acquirer.

What's Covered

- Visa Transaction Processing—Who is Involved?
- Visa Transaction Flow for Magnetic-Stripe and Chip Cards
- Visa Transaction Flow for PIN-Based Point-of-Sale and ATM
- Cardholder Disputes and Chargebacks
- Visa Rules
- Visa Rules for Returns and Exchanges

By accepting Visa cards at your point-of-sale, you become an integral part of the Visa payment system. That's why it's important that you start with a clear picture of the Visa card transaction process; what it is, how it works, and who's involved. The basic knowledge in this section provides you with a conceptual framework for the policies and procedures applicable to a Visa merchant. It will also help you to understand the major components of payment processing and how they affect the way you do business.

Visa Transaction Processing—Who is Involved?

Parties to Visa Transactions

Besides you and your customers, several other parties are involved in every Visa transaction. The following summary will help you and your sales staff to better understand who does what.



A cardholder is an authorized user of Visa payment cards or other Visa payment products.



A merchant is any business entity that is authorized to accept Visa cards for the payment of goods and services.



An acquirer is a financial institution that contracts with merchants to accept Visa cards for payment of good and services. An acquirer may also contract with third party processors to provide processing services.



A card issuer is a financial institution that maintains the Visa cardholder relationship. It issues Visa cards and contracts with its cardholders for billing and payment of transactions.



Visa Inc. is a publicly-traded corporation that works with financial institutions that issue Visa cards (card issuers) and/or sign merchants to accept Visa cards for payment of goods and services (acquirers). Visa provides card products, promotes the Visa brand, and establishes the rules and regulations governing participation in Visa programs. Visa also operates the world's largest retail electronic payments network to facilitate the flow of transactions between acquirers and card issuers.



VisaNet® is part of Visa's retail electronic payment system. It is itself a collection of systems that includes:

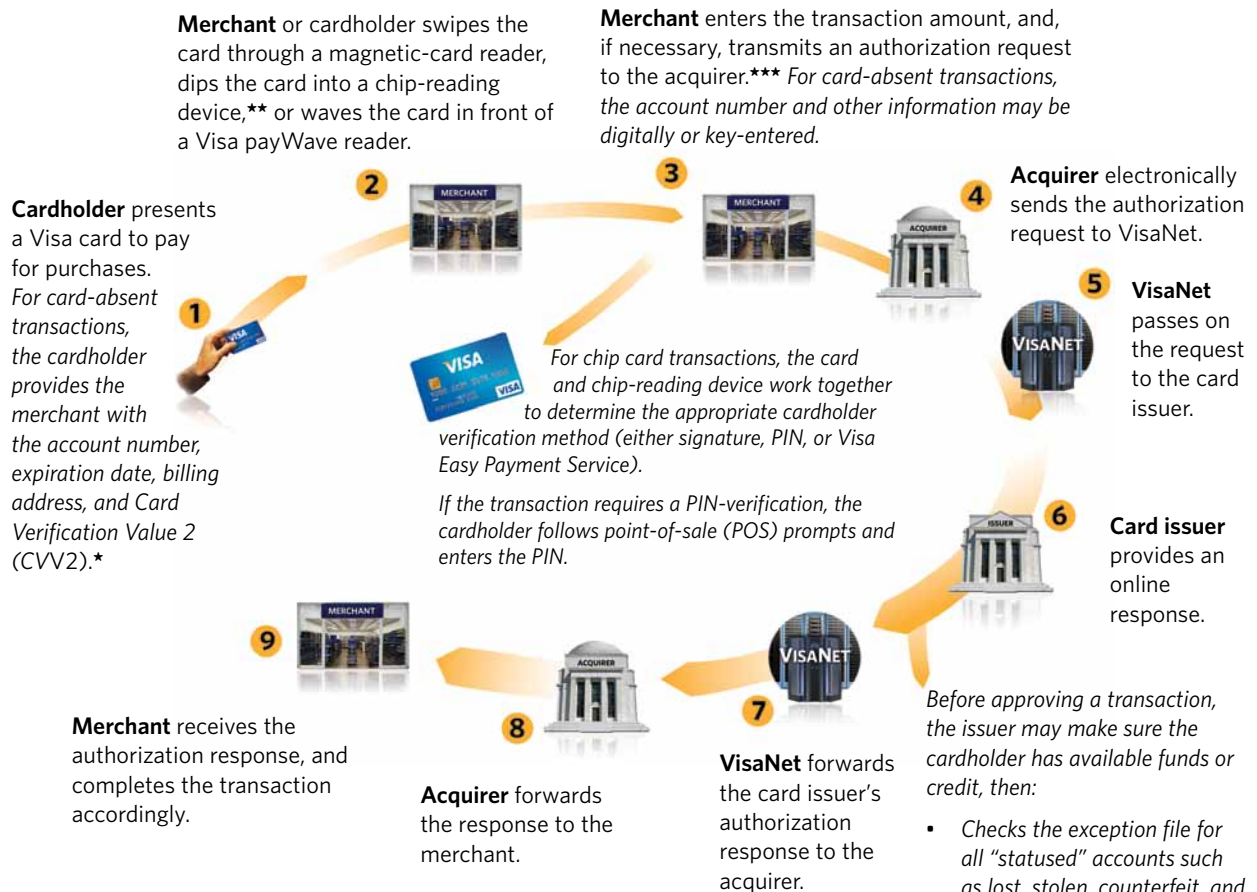
- **An authorization service** through which card issuers can approve or decline individual Visa card transactions.
- **A clearing and settlement service** that processes transactions electronically between acquirers and card issuers to ensure that:
 - Visa transaction information moves from acquirers to card issuers for posting to cardholders' accounts.
 - Payment for Visa transactions moves from card issuers to acquirers to be credited to the merchants' accounts.

Visa Transaction Flow for Magnetic-Stripe and Chip Cards

Transaction Life Cycles

The following illustrations show the life cycle of Visa card transactions for both card-present and card-absent purchases. **Processing events and activities may vary for any particular merchant, acquirer, or card issuer, depending on card and transaction type, and the processing system used.**

Magnetic-Stripe and Chip Card—Credit or Debit Authorization

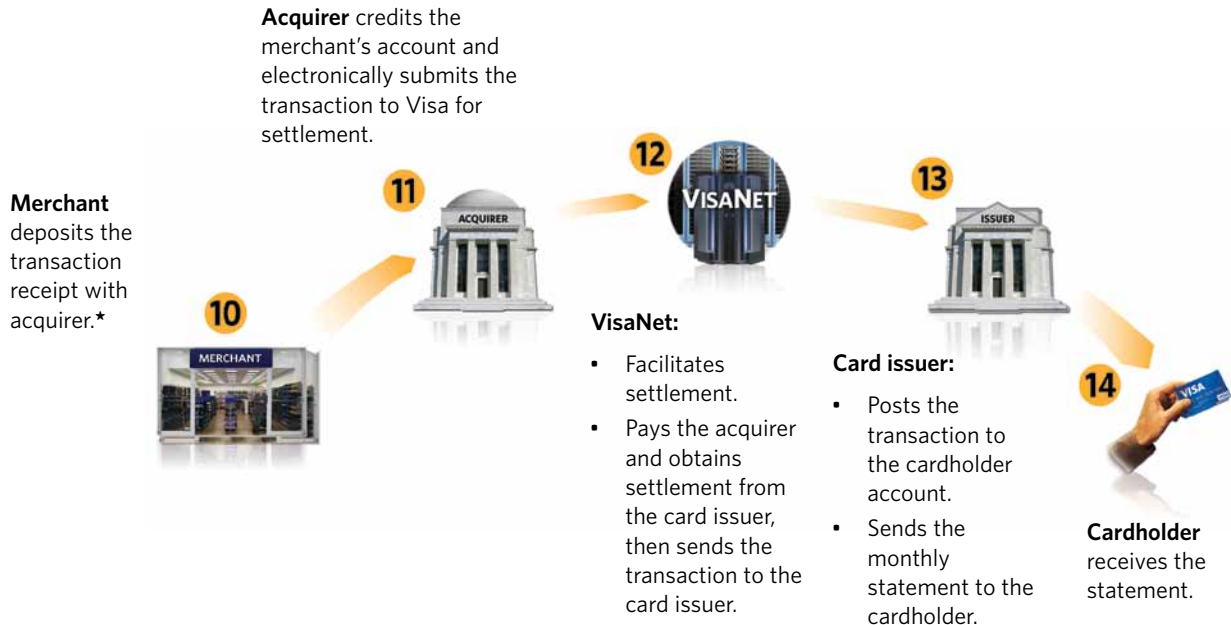


* In certain markets, CVV2 is required to be present for all card-absent transactions.

** Many Visa cards have a chip that communicates information to a POS terminal with a chip-reading device. If a chip reading device is available, preference must always be given to chip card processing before attempting to swipe the stripe.

*** In some markets, chip and Visa payWave allow for chip-based offline authorization.

Magnetic-Stripe and Chip Card—Clearing and Settlement

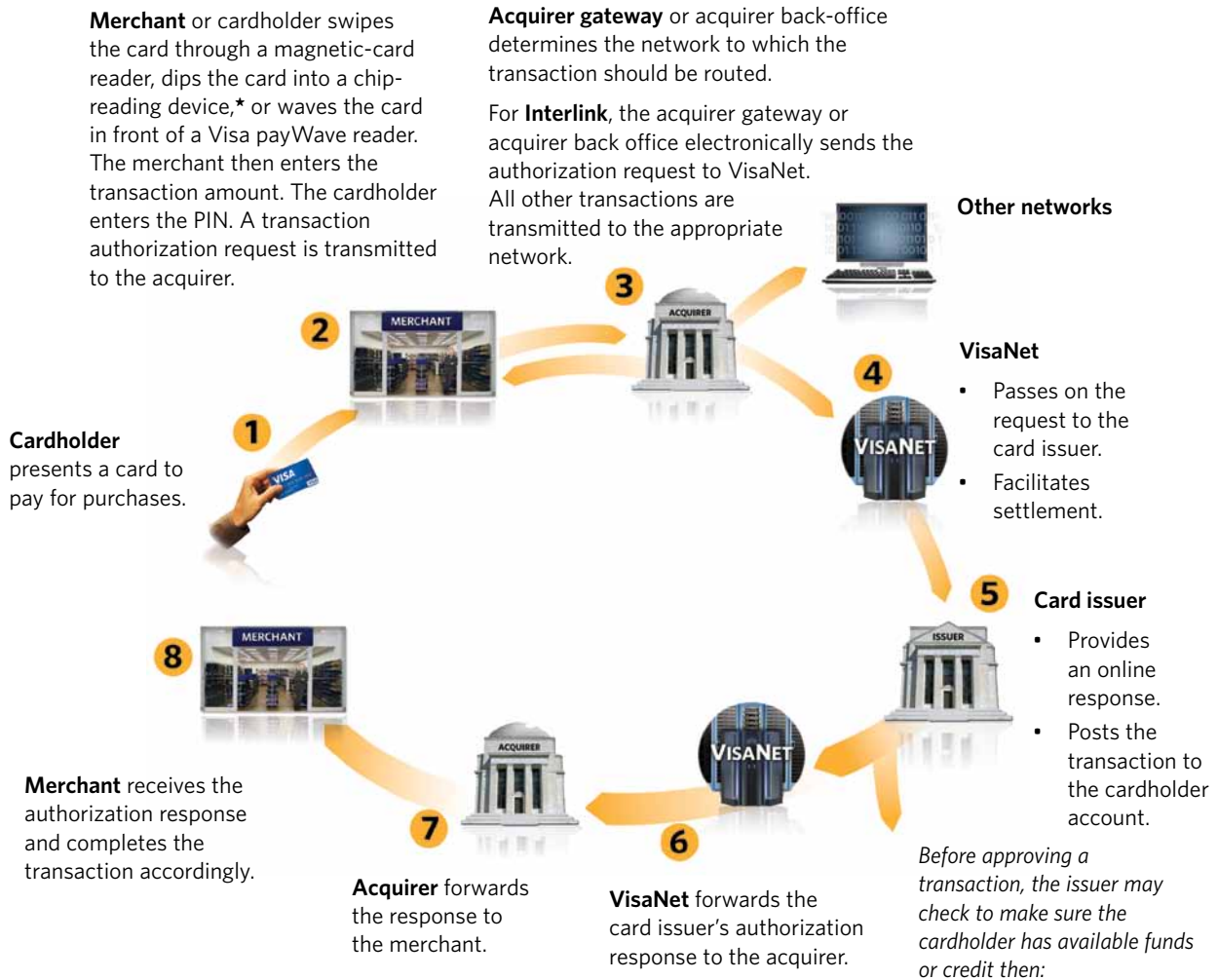


* Merchants or their Third Party Agents that store, process, or transmit account information may not store sensitive authentication data (full magnetic-stripe or chip), Card Verification Value 2 (CVV2), data, or PIN Verification Value (PVV) data—even if it is encrypted. Once an authorization is processed, such data should no longer exist. The only components of the magnetic stripe or chip that can be stored are the cardholder's name, personal account number (PAN), and expiration date. This information can only be stored if encrypted, suppressed, or masked—as to render it useless in the event of a data breach—in compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Visa Transaction Flow for PIN-Based POS and ATM

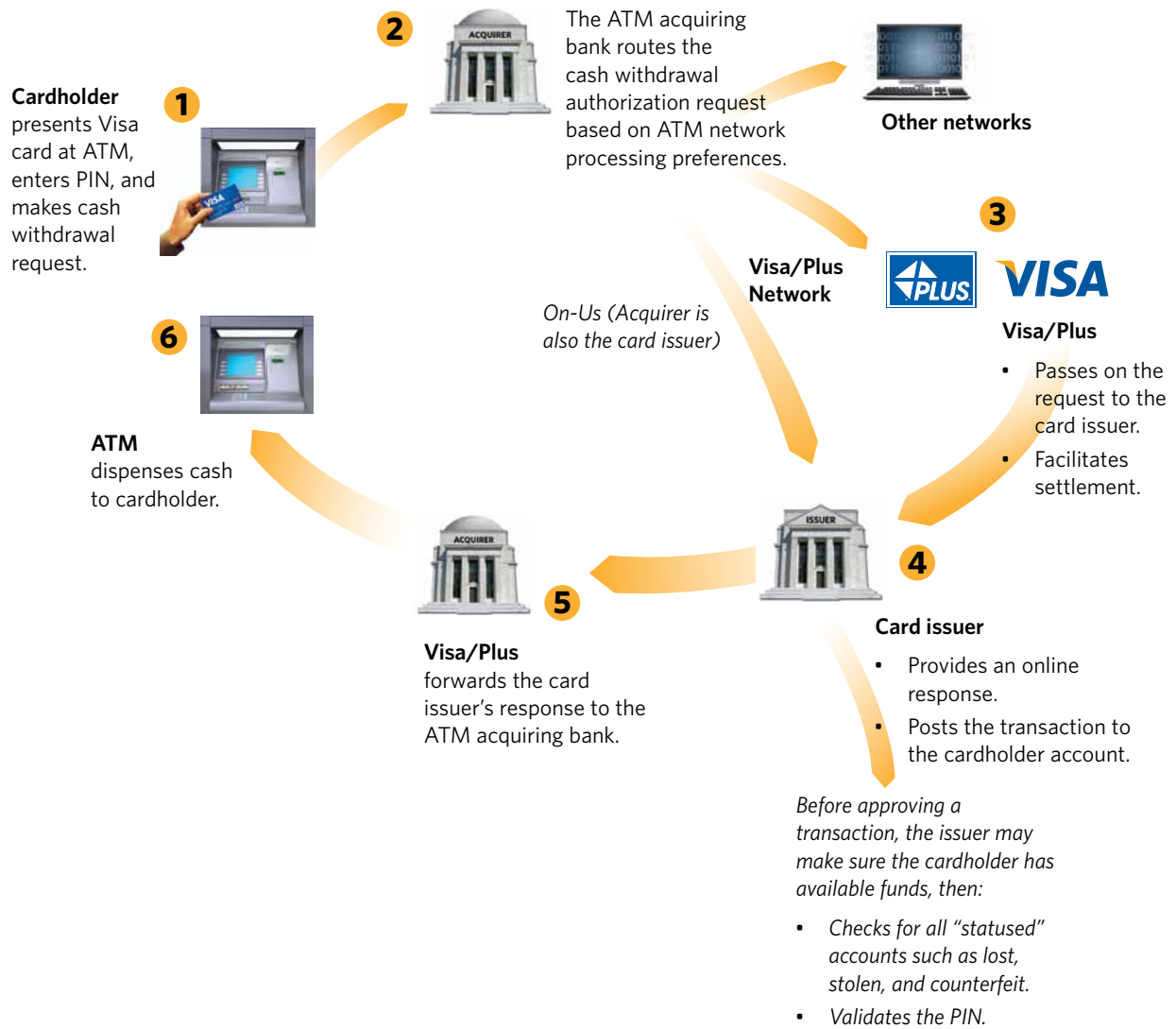
PIN-based POS or ATM transactions are typically authorized and cleared (posted) at the same time within a single message. Settlement occurs from this single message at certain cut-off times during the day. This is referred to as an “online” debit transaction. The following diagrams illustrate the basic processing steps for PIN-based POS (Interlink) and ATM (Visa/Plus) transactions.

Interlink Authorization, Clearing and Settlement



* Many Visa cards have a chip that communicates information to a point-of-sale terminal with a chip-reading device. If a chip reading device is available, preference must always be given to chip card processing before attempting to swipe the stripe.

Visa/Plus Authorization, Clearing and Settlement



Cardholder Disputes and Chargebacks

What is a Chargeback?

A “chargeback” provides an issuer with a way to return a disputed transaction. When a cardholder disputes a transaction, the issuer may request a written explanation of the problem from the cardholder and can also request a copy of the related sales transaction receipt from the acquirer, if needed. Once the issuer receives this documentation, the first step is to determine whether a chargeback situation exists. There are many reasons for chargebacks—**those reasons that may be of assistance in an investigation include the following:**

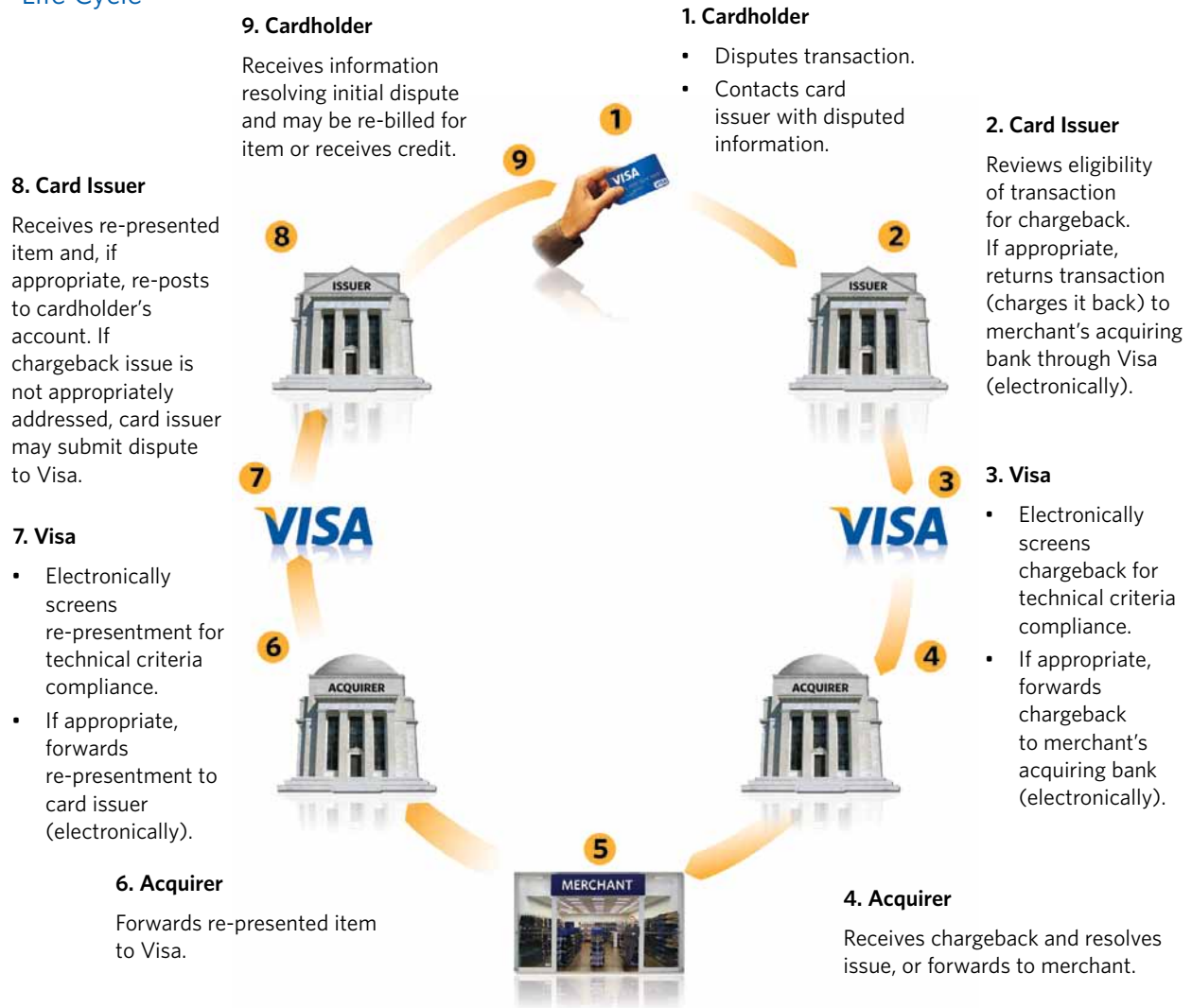
- Merchant failed to get an authorization
- Transaction receipt is altered or unsigned (or PIN not obtained)
- Merchant failed to obtain card imprint (electronic or manual)
- Merchant accepted an expired card

When a chargeback right applies, the issuer sends the transaction back to the acquirer and charges back the dollar amount of the disputed sale. The acquirer then researches the transaction. If the chargeback is valid, the acquirer deducts the amount of the chargeback from the merchant account and informs the merchant.

Under certain circumstances, a merchant may re-present the chargeback to its acquirer. If the merchant cannot remedy the chargeback, it is the merchant’s loss. If there are no funds in the merchant’s account to cover the chargeback amount, the acquirer must cover the loss.

The Chargeback Life Cycle

The following illustration shows the chargeback life cycle.



Arbitration

If the card issuer disputes a representation from the acquirer, the card issuer may file for arbitration with Visa. In arbitration, Visa decides which party is responsible for the disputed transaction. In most cases, Visa's decision is final and must be accepted by both the card issuer and the acquirer. During arbitration, Visa reviews all information/documentation submitted by both parties to determine who has final liability for the transaction.

Compliance

Members may submit a compliance case to Visa for review if members incur a loss and a valid chargeback or representation is unavailable.

Visa Rules

Merchants must follow basic card acceptance rules for all Visa transactions. Careful and consistent adherence to the Visa rules outlined in this section will help you to enhance customer satisfaction and operate your business efficiently. If you have any questions about any of the Visa rules presented here, contact your acquirer.

Taxes

Include tax in the total transaction amount. Any tax that you are required to collect must be included in the total transaction amount. Never collect taxes separately in cash.

Card Acceptance

Accept all types of valid Visa cards. Although Visa card acceptance rules may vary based on country-specific requirements or local regulations, to offer the broadest possible range of payment options to cardholder customers, most merchants choose to accept all categories of Visa debit, credit, and prepaid cards.*

Minimum/Maximum Purchase



Check with your acquirer regarding the minimum purchase amount that you are allowed to charge. U.S. merchants may establish a minimum purchase amount on credit card transactions. The minimum purchase amount must not exceed \$10, must not differentiate between card issuers or card brand, and does not apply to transactions made with a debit card.



Adhere to any maximum purchase amounts on credit card transactions established by federal agencies or institutions of higher education. The maximum purchase amount must not differentiate between card issuers or card brand, and does not apply to transactions made with a debit card.



In other countries, there are multiple variations of the “Minimum Purchase” rule, depending on local law and acquiring practices. Your acquirer can advise you regarding permissible minimum purchase amounts.

No Surcharging

Always treat Visa transactions like any other transaction. You must not impose any surcharge** on a Visa transaction.

Prohibited Uses

Never use the Visa card/account number to refinance existing debts or as a payment for a debt deemed as uncollectible (i.e., recover funds for a dishonored check).

Quick Tip



When prominently displayed, Visa decals and point-of-sale signage are helpful tools for encouraging your customers to use their Visa cards to pay.

* Visa debit and credit cards may have different acceptance policies if you are located in the U.S., Australia, or Canada.

** There are certain variations of the “No Surcharging” rule, depending on local law and acquiring practices. Check with your acquirer regarding prohibited surcharges and/or discounts.

Convenience Fees*



For merchants who offer an alternate payment channel (i.e., mail, telephone, or e-commerce) for customers to pay for goods or services, a convenience fee may be added to the transaction amount. If the merchant chooses to assess a convenience fee to its customers, the merchant **must** adhere to Visa rules regarding convenience fees.

For further information on Convenience Fees, please contact your acquirer.

Laundering

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

Zero-Percent Tip



For restaurant, taxicab, limousine, bar, tavern, beauty/barber shop, and health/beauty spa merchant transactions with a Visa credit or debit card, authorize only for the known amount, not the transaction amount plus estimated tip.

Cardholders now have the ability to check their credit or checking accounts almost instantaneously via phone, the Internet, or an ATM. 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, a restaurant authorizes for an estimated 20 percent tip, but the customer adds on only 15 percent.

If the exact amount of the tip is known at the time of authorization, then it should be included in the authorization amount. This is common for chip and PIN transactions.



Restaurant, taxicab, limousine, bar, tavern, beauty/barber shop, and health/beauty spa authorizations are valid for the transaction amount plus or minus 20 percent to protect merchants from chargeback liability for failure to obtain proper authorization.



Restaurants are permitted and protected from chargeback for failure to obtain proper authorization if they clear for an amount up to 20 percent more than they authorized, and the same is true up to 15 percent additional for T&E merchants.

For further information on zero-percent tip authorization, contact your acquirer.

* Visa Convenience Fees are permitted only under certain circumstances in the U.S., CEMEA, and Asia Pacific.

No Cash Refunds

Complete a Visa credit receipt for merchandise returns or adjustments. Do not provide cash refunds for returned merchandise originally purchased with a Visa card. Visa does not permit 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 Visa account and then return the merchandise for cash.

If a transaction was conducted with a Visa prepaid card and the cardholder is returning items but has discarded this card, you may give a cash refund or in-store credit.

Deposit Time Limits

Deposit your Visa transaction receipt as specified by your acquirer. Generally, transaction receipts must be deposited within three business days of the transaction date, with some exceptions. The sooner you deposit transaction receipts with your acquirer, the sooner you get paid. Transactions deposited more than 30 days after the original transaction date may be charged back to you. For card-absent transactions, the transaction date is the merchandise **ship date**, not the order date.

Suppressed Account Number and Expiration Date

Ensure that the Visa account number is suppressed in accordance with Visa rules and local laws and regulations. Visa recommends that all but the last four digits of the account number be suppressed on the cardholder copy of the transaction receipt, unless otherwise required under local law.

The expiration date should not appear at all on the cardholder copy of the transaction receipt. Existing point-of-sale terminals must comply with these requirements. To ensure that your point-of-sale terminals are properly set up for account number and expiration date suppression, contact your acquirer.

Delivery of Goods and Services

Deliver the merchandise or services to the cardholder at the time of the transaction. Cardholders expect immediate delivery of goods and services unless other delivery arrangements have been made. For card-absent transactions, cardholders should be informed of delivery method and tentative delivery date. Transactions cannot be deposited until goods or services have been shipped.

Delayed Delivery

For a delayed delivery, obtain where applicable two authorizations: one for the deposit amount and one for the balance amount. Some merchandise, such as a custom-covered sofa, requires delivery after the transaction date. In these delayed-delivery situations, the customer pays a deposit at the time of the transaction and agrees to pay the balance upon delivery of the merchandise or services.

To complete a delayed-delivery transaction, you should where applicable:

- **Create two transaction receipts**, one for the deposit and one for the balance. Write, print out, or stamp “Deposit” or “Balance,” as appropriate, on the receipt.
- **Obtain an authorization** for each transaction receipt on their respective transaction dates. Ensure an authorization code is on each receipt; if your point-of-sale device does not automatically print authorization codes on sales receipts, write the codes on the receipts so they are clearly identifiable as such.
- **Ensure that “Delayed Delivery”** is written, printed, or stamped along with the authorization code, on each transaction receipt.

You may deposit the deposit portion of the transaction before delivery of the goods or services. However, you must **not** deposit the balance portion of the transaction amount prior to delivery.

Installment Payments



An installment payment* is a functionality of the credit card. It allows a cardholder to pay the full amount of the transaction in installments. This can be accomplished through interest-bearing financing (granted by the card issuer), allowing the merchant to be paid in one lump sum, or with interest-free financing (granted by the merchant).

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. Keeping that trust is essential to fraud reduction and good customer service. Cardholder account numbers and other personal information should be released only to your acquirer or processor, or as specifically required by law.



For more information on Visa’s data security requirements and programs, see *Section 4: Payment Card Industry Data Security Standard and PIN Security and Key Management in Card Acceptance Guidelines for Visa Merchants*. To obtain a copy of this publication contact your acquirer.

* Installment payments apply only in Asia Pacific and Latin America.

Merchant Servicer Registration

Merchants and their Visa acquirers must ensure that Third Party Agents who are handling Visa account numbers are registered in accordance with the *Visa International Operating Regulations*. A merchant servicer (MS) is defined by Visa as a Third Party Agent that has a direct relationship with a merchant and is storing, processing or transmitting Visa account numbers on the merchants' behalf. This type of Third Party Agent performs services such as payment gateway, shopping cart, fraud scrubbing, loyalty programs, etc. Merchants and their Visa acquirers are responsible for ensuring each MS maintains compliance with the Payment Card Industry (PCI) Data Security Standard (DSS), validates PCI DSS compliance with Visa, and is correctly registered as a MS with Visa.

Merchants should work with their Visa acquirers to ensure all Third Party Agent rules and requirements have been satisfied, ensuring the merchants compliance with *Visa International Operating Regulations*.

Any Third Party Agent that is used by a merchant must be validated for PCI DSS compliance and listed on Visa's validated service providers list. The global list of PCI DSS Validated Service Providers is located on www.visa.com/cisp.



For more information on Visa's data security requirements and programs, see *Section 4: Payment Card Industry Data Security Standard and PIN Security and Key Management in Card Acceptance Guidelines for Visa Merchants*. To obtain a copy of this publication contact your acquirer.

Sensitive Data Storage and Payment Application Use

All stored, processed or transmitted sensitive cardholder account or transaction information must comply with the PCI DSS and the *Visa International Operating Regulations*. To protect sensitive customer and transaction information from compromise merchants that store, process, or transmit cardholder account or transaction data must:

- Keep all material containing account numbers—whether on paper or electronically—in a secure area accessible to only selected personnel. Merchants with paper receipts should be extremely careful during the storage or transfer of this sensitive information. Merchants should at all times:
 - Promptly provide the drafts to their acquirer.
 - Destroy all copies of the drafts that are not delivered to the acquirer.
- Render cardholder data unreadable, both in storage and prior to discarding.
- Never retain full-track, magnetic-stripe, CVV2*, and chip data subsequent to transaction authorization. Storage of track data elements in excess of name, personal account number (PAN), and expiration date after transaction authorization is strictly prohibited.
- Use payment applications that comply with the PCI Payment Application Data Security Standard (PA-DSS). A list of validated payment applications is available at www.pcissc.org.

* In certain markets, CVV2 is required to be present for all card-absent transactions.

Visa Rules for Returns and Exchanges

As a merchant, you are responsible for establishing your merchandise return and adjustment (credit) policies. Clear disclosure of these policies can help you avoid misunderstandings and potential cardholder disputes. Visa will support your policies, provided they are clearly disclosed to cardholders **before** the completion of a transaction.

If you are unsure how to disclose your return and adjustment policies, contact your acquirer for further guidance.

Disclosure for Card-Present Merchants

For card-present transactions, Visa will accept that proper disclosure has occurred before a transaction is completed if the following (or similar) disclosure statements are legibly printed on the face of the transaction receipt near the cardholder signature line.

Disclosure Statement	What It Means
No Refunds, Returns, or Exchanges	Your establishment does not issue refunds and does not accept returned merchandise or merchandise exchanges.
Exchange Only	Your establishment is willing to exchange returned merchandise for similar merchandise that is equal in price to the amount of the original transaction.
In-Store Credit Only	Your establishment takes returned merchandise and gives the cardholder an in-store credit for the value of the returned merchandise.
Special Circumstances	You and the cardholder have agreed to special terms (such as late delivery charges or restocking fees). The agreed-upon terms must be written on the transaction receipt or a related document (e.g., an invoice). The cardholder's signature on the receipt or invoice indicates acceptance of the agreed-upon terms.
Timeshare	You must provide a full credit when a transaction receipt has been processed and the cardholder has cancelled the transaction within 14 calendar days of the transaction date.

Disclosure for
Card-Absent
Merchants

Mail Order

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

Internet

Your website must communicate its refund policy to the cardholder and require the cardholder to select a “click-to-accept” or other affirmative button to acknowledge the policy. The terms and conditions of the purchase must be displayed on the same screen view as the checkout screen that presents the total purchase amount, or within the sequence of website pages the cardholder accesses during the checkout process.

Section 2 Copy Requests

What's Covered

- Transaction Receipt Requirements—Card-Present Merchants
- Transaction Receipt Requirements—Card-Absent Merchants
- Responding to Copy Requests
- How to Minimize Copy Requests

When cardholders do not recognize transactions on their Visa statements, they typically ask their card issuer for a copy of the related transaction receipt to determine whether the transaction is theirs. In this kind of situation, the card issuer first tries to answer the cardholder's questions. If this cannot be done, the card issuer electronically sends a "request for copy" (also known as a "retrieval request") to the acquirer associated with the transaction.

If your transaction receipts are stored at your acquirer, the acquirer will fulfill the copy request. However, if you store your own transaction receipts, the acquirer forwards the request to you. You must then send a legible copy of the transaction receipt to the acquirer. The acquirer will send it on to the card issuer.

This section highlights merchant requirements and best practices for responding to a request for a copy of a sales receipt.

Note: Copy requests are no longer required for chip card, EMV PIN (except in the case of T&E document requests, cash and quasi-cash transactions), and VEPS transactions. As a result:

- Issuers no longer need to process a copy request for a chip card, EMV PIN, and VEPS transaction dispute before initiating a chargeback.
- If a copy request is received for a chip-read transaction, the acquirer no longer needs to fulfill the request.

Transaction Receipt Requirements—Card-Present Merchants

The following are the Visa requirements for all transaction receipts generated from electronic point-of-sale terminals (including cardholder-activated terminals).

Electronic Point-of-Sale Terminal Receipts

Transaction Date

Merchant Location Code

The payment brand used to complete the transaction must be identified on the cardholder's copy of the transaction receipt.

Authorization Code, if applicable, except for Visa Easy Payment Service (VEPS).

Space for Cardholder Signature, except for:

- Transactions in which the PIN is an acceptable substitute for cardholder signature
- Limited-Amount Terminal Transactions
- Self-Service Terminal Transactions
- VEPS

Merchant or member name and location, or the city and state of the Automated Dispensing Machine or Self-Service Terminal

XYZ SHOES
1040 PARK ST
ANYTOWN, CA 94501
PHONE # (000)555-5555
MAY 10, 2010 12:30PM

MERCH ID: 08233004

REF # : 003
CT # : *****5220
EXP : XX/XX
CARD : VISA

\$21.69

APPROVAL CODE: 035789
TRAN ID: VGT7ET800815

X _____
SIGNATURE

No refunds after 30 days.

THANK YOU
CARDHOLDER COPY

Suppressed Account Number
Visa recommends that all but the last four digits of the account number on the cardholder copy of the transaction receipt be suppressed.

In addition, the **Expiration Date** should not appear at all. To ensure your point-of-sale terminals are properly set up for account number suppression, contact your acquirer.

Transaction Amount

Refund/Return Policy (optional)

Transaction Receipt Requirements—Card-Absent Merchants

The following are the Visa requirements for all manually printed transaction receipts in the card-absent environment.

Manual Transaction Receipts

Merchant Name and Location

Merchant Online Address

Payment Method Used

Transaction Type: Purchase or Credit

Books Are Us 1111 Something Ave. City, State 98102 Order placed: April 14, 2010 www.booksareus.com		Transaction Date	
Description of Goods or Services			
ORDER #: 103-62567-3299874			
Shipping Address: John Bennett 2423 Sweet Dr. San Francisco, CA 94111 USA	Items Ordered 1 How to Raise a Puppy (Hardcover) by Jane Russo - 1 item(s) Gift options: None	Price \$16.95	
Shipping: Standard	Item(s) Subtotal: \$16.95 Shipping & Handling: \$3.99 Subtotal: \$20.64 Total for this Shipment: \$20.64		
PAYMENT INFORMATION Printable version			
Payment Method: Visa Last 4 digits: 0123 Authorization Code: XXXXXX Transaction Type: Purchase	Authorization Code		
Billing Address: John Bennett 1111 Sweet Dr. San Francisco, CA 94111 USA	Item(s) Subtotal: \$16.95 Shipping & Handling: \$3.99 Total Before Tax: \$20.64 Estimated Tax: \$0.00 Grand Total: \$20.64		
No refunds after 30 days. See our Return Policy. Questions? Call Customer Service at 1-800-111-1111			

Refund/Return Policy (optional)

Transaction Amount

Responding to Copy Requests

The illustration on the next page shows the copy request process. When a card issuer sends a copy request to an acquirer, the bank has 30 days from the date it receives the request to send a copy of the sales receipt back to the card issuer. If the acquirer sends the request to you, it will tell you the number of days you have to respond. You must follow the acquirer's time frame.

Once you receive a copy request, retrieve the appropriate sales receipt, make a legible copy of it, and fax or mail it to your acquirer within the specified time frame. Your acquirer will then forward the copy to the card issuer, which will, in turn, send it to the requesting cardholder. The question or issue the cardholder had with the transaction is usually resolved at this point.

Note: When you send the copy to the acquirer, use a delivery method that provides proof of delivery. If you mail the copy, send it by registered or certified mail. If you send the copy electronically, be sure to keep a written record of the transmittal.



If you store your own sales receipts, you should retain your merchant copies—or copies of them, for example, on CD-ROM—for 13 months from the date of the original transaction to ensure your ability to fulfill copy requests.

Copy Requests by Phone

To assist their cardholders, card issuers may call you directly to request a copy of a sales receipt. You are not obligated to fulfill a verbal copy request from a card issuer. However, if you do decide to provide a copy of the sales receipt, be sure to keep a copy for your own records. You may find you need it for dispute-related or accounting purposes.

It Pays to Respond to Copy Requests

Responding to copy requests saves you time and money. As a merchant, you should always:

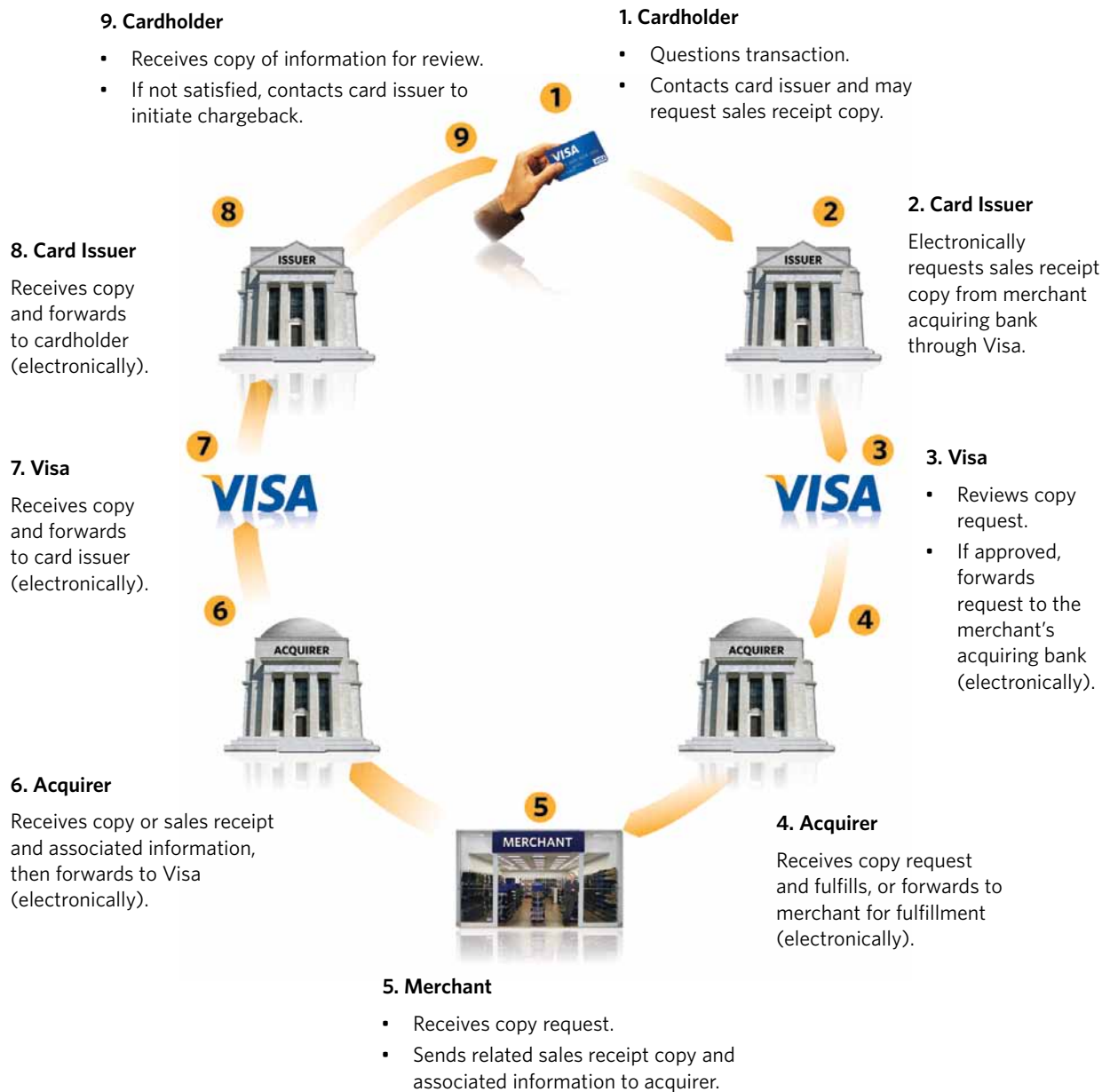
- Fulfill any copy requests you receive, except for chip card, EMV PIN (except in the case of T&E document requests, cash and quasi-cash transactions), and VEPS transactions where the merchant is not required to provide copy.
- Fulfill requests in a timely manner.
- Ensure that the receipt copy you send is legible.
- Provide transaction details that may assist the cardholder in recognizing the transaction.

Avoiding chargebacks can help you improve your customer service.

Card-Present Merchants

If the copy request you receive from an issuer is for a card-present transaction, you are required to provide a **legible copy of an original transaction receipt**. A substitute transaction receipt is considered invalid. The copy you provide must be legible and should contain proof the card was present and have a signature. **Responding to a copy request without these key elements may result in a chargeback and you may incur financial liability for the disputed amount. (See *Minimizing Chargebacks* in Section 3: Chargebacks.)**

The Copy Request Process



How to Minimize Copy Requests

Merchants who keep copy requests to a minimum are more likely to have lower chargeback rates. Best practices for reducing copy requests include:

Make Sure Customers Can Recognize Your Name on Their Bills

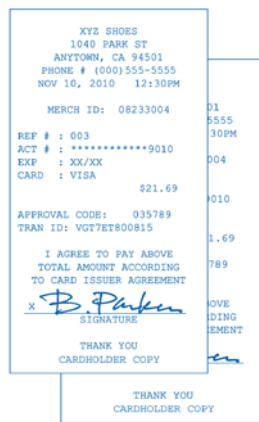
Cardholders must be able to look at their bank statements and recognize transactions that occurred at your establishment. Check with your acquirer to be sure it has the correct information on your “Doing Business As” (DBA) name, city, and state/region/province. You can check this information yourself by purchasing an item on your Visa card at each of your outlets and looking at the merchant name and location on your monthly Visa statement. Is your name recognizable? Can your customers identify the transactions made at your establishment?

Make Sure Your Business Name Is Legible on Receipts

Make sure your company’s name is accurately and legibly printed on transaction receipts. The location, size, or color of this information should not interfere with transaction detail. Similarly, you should make sure that any company logos or marketing messages on receipts are positioned away from transaction information.



Handle carbonless paper and carbon/silver-backed paper carefully



Keep white copy of sales draft receipt—give customers colored copy



Change point-of-sale printer cartridge routinely



Change point-of-sale printer paper when colored streak first appears

Train Sales Staff

With proper transaction processing, many copy requests can be prevented at the point of sale. Instruct your sales staff to:

- Follow proper point-of-sale card acceptance procedures.
- Review each transaction receipt for accuracy and completeness.
- Ensure the transaction receipt is readable. (See *Minimizing Chargebacks in Section 3: Chargebacks.*)
- Give the cardholder the customer copy of the transaction receipt, and keep the original, signed copy.

Sales associates should also understand that merchant liability encompasses the merchandise, as well as the dollar amount printed on the receipt; that is, in the event of a dispute, the merchant could lose both.

Avoid Illegible Transaction Receipts

Ensuring legibility of transaction receipts is key to minimizing copy requests and chargebacks. When responding to a copy request, you will usually photocopy or scan the transaction receipt before mailing or electronically sending it to your acquirer. If the receipt is not legible to begin with, the copy that the acquirer receives and then sends to the card issuer may not be useful in resolving the cardholder's question. If this occurs, the transaction may be returned to you as a chargeback for an illegible copy. At this point, unless you can improve the readability of the transaction receipt, you may end up taking a loss on the transaction.

The following best practices are recommended to help avoid illegible transaction receipts.

- **Change point-of-sale printer cartridge routinely.**
Faded, barely visible ink on transaction receipts is the leading cause of illegible receipt copies. Check readability on all printers daily and make sure the printing is clear and dark on every sales draft.
- **Change point-of-sale printer paper when the colored streak first appears.**
The colored streak down the center or on the edges of printer paper indicates the end of the paper roll. It also diminishes the legibility of transaction information.
- **Keep the white copy of the transaction receipt.**
If your transaction receipts include a white original and a colored copy, always give customers the colored copy of the receipt. Since colored paper does not photocopy as clearly as white paper, it often results in illegible copies.

- **Handle carbon-backed or carbonless paper carefully.**

Any pressure on carbon-backed or carbonless paper during handling and storage causes black blotches, making copies illegible.

Copy Request Monitoring

Visa recommends that merchants monitor the number of copy requests they receive. If the ratio of copy requests to your total Visa sales (less returns and adjustments) is more than 0.5 percent, you should review your procedures to see if improvements can be made.

What's Covered

- Why Chargebacks Occur
- Customer Dispute Chargebacks
- Invalid Chargebacks
- Minimizing Chargebacks
- Chargeback Monitoring
- When Chargeback Rights Do Not Apply

A chargeback is a transaction that a card issuer returns to an acquirer as a financial liability and which, in turn, an acquirer may return to a merchant. In essence, it reverses a sales transaction:

- The card issuer subtracts the transaction dollar amount from the cardholder's Visa account. The cardholder receives a credit and is no longer financially responsible for the dollar amount of the transaction.
- The card issuer submits a chargeback through VisaNet to the acquirer for the dollar amount of the transaction.
- The acquirer 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 can also incur your own internal costs for processing the chargeback. Since you control how your employees handle transactions, you can prevent many unnecessary chargebacks by simply training your staff to pay attention to a few details.

In this section, you will find a set of strategies for chargeback prevention, as well as information on how and when to resubmit a charged-back transaction to your acquirer. A brief compliance process overview is also included.

Why Chargebacks Occur

Four Common Reasons

The most common reasons for chargebacks include:

- Customer disputes
- Fraud
- Processing errors
- Authorization issues

Although you probably cannot avoid chargebacks completely, you can take steps to reduce or prevent them. Many chargebacks result from 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 *Minimizing Chargebacks* in this section.)

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



Your Responsibility

From the administrative point of view, the main interaction in a chargeback is between a card issuer and an acquirer. The card issuer sends the chargeback to the acquirer, which may or may not need to involve the merchant who submitted the original transaction. This processing cycle does **not** relieve merchants of the responsibility of taking action to remedy and prevent chargebacks. In most cases, the full extent of your financial and administrative liability for chargebacks is spelled out in your merchant agreement.



For more information on the most common types of chargebacks merchant receive, see *Section 4, Chargeback Reason Codes*.

Customer Dispute Chargebacks

Customer disputes are one of the most common reasons for chargebacks.

A customer may dispute a transaction because:

- A credit has not been processed when the customer expected it would be.
- Merchandise ordered was never received.
- A service was not performed as expected.
- The customer did not make the purchase; it was fraudulent.

Because these chargebacks may indicate customer dissatisfaction—and the potential for lost sales in the future—addressing their underlying causes should be an integral part of your customer service policies.

Invalid Chargebacks

Responding to the needs of card issuers, acquirers, and merchants, Visa has implemented sophisticated systems that significantly reduce chargebacks and vastly improve the chargeback process. When Visa systems detect an invalid chargeback, it is automatically returned to the card issuer that originated it, and the merchant and acquirer never see it. Many acquirers also have systems that routinely review exception items, allowing them to resolve issues before a chargeback is necessary. Together, these systems ensure that chargebacks you receive are either those that only you can respond to or those that cannot be remedied in any other way.



If a cardholder with a valid dispute contacts you directly, act promptly to resolve the situation. Issue a credit, as appropriate, and send a note or e-mail message to let the cardholder know he or she will be receiving a credit.

Minimizing Chargebacks

Even when you do receive a chargeback, you may be able to resolve it without losing the sale. Simply provide your acquirer with additional information about the transaction or the actions you have taken related to it. For example, you might receive a chargeback because the cardholder is claiming that credit has not been given for returned merchandise. You may be able to resolve the issue by providing proof that you submitted the credit on a specific date. Send this information to your acquirer in a timely manner.

The key in this, and similar situations, is always send your acquirer as much information as possible to help it remedy the chargeback. With appropriate information, your acquirer may be able to resubmit, or “re-present,” the item to the card issuer for payment.

Timeliness is also essential when attempting to remedy a chargeback. Each step in the chargeback cycle has a defined time limit during which action can be taken. If you or your acquirer do not respond during the time specified on the request—which may vary depending on your acquirer—you will not be able to remedy the chargeback.

Although many chargebacks are resolved without the merchant losing the sale, some cannot be remedied. In such cases, accepting the chargeback may save you the time and expense of needlessly contesting it.

Most chargebacks 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.

Card-Present Merchants

- **Declined Authorization.** Do not complete a transaction if the authorization request was declined. Do not repeat the authorization request after receiving a decline. Instead, ask for another form of payment.
- **Transaction Amount.** Do not estimate transaction amounts. For example, restaurant merchants should authorize transactions only for the known amount on the check; they should not add on a tip.
- **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. In such instances, be prepared to answer questions. The operator may ask to speak with the cardholder. If the transaction is approved, write the authorization code on the sales receipt. If declined, ask the cardholder for another Visa card.

Failure to respond to a referral request may result in a lost sale if a cardholder does not have an alternate means to pay.

- **Expired Card.** Do not accept a card after its “Good Thru” or “Valid Thru” date.

- **Missing or Questionable Cardholder Signature.** In the card-present environment, the cardholder's signature is required for all magnetic-stripe and some chip transactions. For example, a card and signature is required if Card Verification Method (CVM) is signature preferring, except for qualified VEPS transactions. Failure to obtain the cardholder's signature could result in a chargeback if the cardholder denies authorizing or participating in the transaction. When checking the signature, always compare the first letter and spelling of the surname on the sales receipt with the signature on the card. If they are not the same, ask for additional identification or make a Code 10 call.



A chip card and the chip-reading device work together to determine the appropriate cardholder or verification method for transaction (either signature or PIN). If the transaction has been PIN verified, there is no need for signature.

- **Card Imprint for Key-Entered Card-Present Transactions.** 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. Do not capture an impression of the card using a pencil, crayon, or other writing instrument. This process does not constitute a valid imprint. Even if the transaction is authorized and the receipt is signed, the transaction may be charged back to you if fraud occurs and the receipt does not have an imprint of the embossed account number and expiration date.

This applies to all card-present transactions, including key-entry situations where the card presented is chip and the terminal is chip-enabled. When a merchant key-enters a transaction, an imprint is required regardless of the type of card and terminal capability.

- **Legibility.** Ensure that the transaction information on the sales receipt is complete, accurate, and legible before completing the sale. An illegible receipt, or a receipt which produces an illegible copy, may be returned because it cannot be processed properly. The growing use of electronic scanning devices for the electronic transmission of copies of sales receipts makes it imperative that the item being scanned be very legible.
- **Digitized Cardholder Signature.** Some Visa cards have a digitized cardholder signature on the front of the card in addition to the hand-written signature on the signature panel on the back. Checking the digitized signature is not sufficient for completing a transaction. Sales staff must always compare the customer's signature on the sales receipt with the hand-written signature in the signature panel.
- **Fraudulent Card-Present Transaction.** If the cardholder is present and has the account number but not the card, do not accept the transaction. Even with an authorization approval, the transaction can be charged back to you if it turns out to be fraudulent.



"No Chargeback" Sales Receipts

Independent entrepreneurs have been selling sales-receipt stock bearing a statement near the signature area that the cardholder waives the right to charge the transaction back to the merchant. These receipts are being marketed to merchants with the claim that they can protect businesses against chargebacks; in fact, they do not. "No chargeback" sales receipts undermine the integrity of the Visa payment system and are prohibited.

Card-Absent Merchants

Address Verification Service (AVS)* and Card Verification Value 2 (CVV2)** Chargeback Protection



Card-absent merchants should be familiar with the chargeback representment rights associated with the use of AVS and CVV2 and the option to provide compelling information. **Specifically, your acquirer can represent a charged-back transaction if:**

- You received an AVS positive match “Y” response in the authorization message and if the billing and shipping addresses are the same. You will need to submit proof of the shipping address and **signed** proof of delivery.
- You submitted an AVS query during authorization and received a “U” response from a card issuer. This response means the card issuer is unavailable or does not support AVS.
- You submitted a CVV2 verification request during authorization and received a “U” response with a presence indicator of 1, 2, or 9 from a card issuer. This response means the card issuer does not support CVV2.
- You can provide documentation that you:
 - Spoke to the cardholder and he or she now acknowledges the validity of the transaction, **or**
 - Received a letter or e-mail from the cardholder that he or she now acknowledges the validity of the transaction.

If you believe you have AVS, CVV2, or compelling information representment rights on a charged-back transaction, work with your acquirer to ensure that all supporting evidence for the representment is submitted.

Verified by Visa Chargeback Protection

Verified by Visa provides cardholder authentication for online transactions. Based on the 3-D Secure protocol, the Verified by Visa service validates the authenticity of cardholders to participating merchants. It allows cardholders to choose a password through their card issuer, and use it to authenticate themselves while making a purchase. This helps ensure that their card number cannot be fraudulently used on the merchant’s Internet website.

* AVS is only available in the U.S. and Canada.

** In certain markets, CVV2 is required to be present for all card-absent transactions.

Verified by Visa participating merchants are protected by their acquirer from receiving certain fraud-related chargebacks, provided the transaction is processed correctly.

If:	Then:
The cardholder is successfully authenticated	The merchant is protected from fraud-related chargebacks, and can proceed with authorization using Electronic Commerce Indicator (ECI) of '5'.*
The card issuer or cardholder is not participating in Verified by Visa	The merchant is protected from fraud-related chargebacks, and can proceed with authorization using ECI of '6'.*
The card issuer is unable to authenticate	The merchant is not protected from fraud-related chargebacks, but can still proceed with authorization using ECI of '7'. This condition occurs if the card type (i.e., commercial card products) is not supported within Verified by Visa or if the cardholder experiences technical problems.



Liability shift rules for Verified by Visa transactions may vary by region. Please check with your acquirer for further information.

Sales-Receipt Processing

- **One Entry for Each Transaction.** Ensure that transactions are entered into point-of-sale terminals only once and are deposited only once. You may get a chargeback for duplicate transactions if you:
 - Enter the same transaction into a terminal more than once.
 - Deposit both the merchant copy and bank copy of a sales receipt with your acquirer.
 - Deposit the same transaction with more than one acquirer.
- **Voiding Incorrect or Duplicate Sales Receipts.** Ensure that incorrect or duplicate sales receipts are voided and that transactions are processed only once.
- **Depositing Sales Receipts.** Deposit sales receipts with your acquirer as quickly as possible, preferably within one to five days of the transaction date; do not hold on to them.
- **Timely Deposit of Credit Transactions.** Deposit credit receipts with your acquirer as quickly as possible, preferably the same day the credit transaction is generated.

* A Verified by Visa merchant identified by the Merchant Fraud Performance (MFP) program may be subject to chargeback Reason Code 93: Merchant Fraud Performance Program.

Customer Service

- **Delayed Delivery.** If the merchandise or service to be provided to the cardholder will be delayed, advise the cardholder in writing of the delay and the new expected delivery or service date.
- **Item Out of Stock.** If the cardholder has ordered merchandise that is out of stock or no longer available, advise the cardholder in writing. If the merchandise is out of stock, let the cardholder know when it will be delivered. If the item is no longer available, offer the option of either purchasing a similar item or cancelling the transaction. Do not substitute another item unless the customer agrees to accept it.
- **Disclosing Refund, Return, or Service Cancellation Policies.** If your business has policies regarding merchandise returns, refunds, or service cancellation, these policies must be disclosed to the cardholder at the time of the transaction. Your policies should be pre-printed on your sales receipts; if not, write or stamp your refund or return policy information on the sales receipt near the customer signature line before the customer signs (be sure the information is clearly legible on all copies of the sales receipt). Failure to disclose your refund and return policies at the time of a transaction could result in a dispute should the customer return the merchandise.
- **Return, refund, and cancellation policy for Internet merchants.** This policy must be clearly posted to inform cardholders of their rights and responsibilities (e.g., if the merchant has a limited or no refund policy, this must be clearly disclosed on your website before the purchase decision is made to prevent misunderstandings and disputes). The website must communicate its refund policy and require the cardholder to select a “click-to-accept” or other affirmative button to acknowledge the policy. The terms and conditions of the purchase must be displayed on the same screen view as the checkout screen used to present the total purchase amount or within the sequence of website pages the cardholder accesses during the checkout process. This policy page cannot be bypassed.
- **Ship Merchandise Before Depositing Transaction.** For card-absent transactions, do not deposit sales receipts with your acquirer until you have shipped the related merchandise. If customers see a transaction on their monthly Visa statement before they receive the merchandise, they may contact their card issuer to dispute the billing. Similarly, if delivery is delayed on a card-present transaction, do not deposit the sales receipt until the merchandise has been shipped.
- **Requests for Cancellation of Recurring Transactions.** If a customer requests cancellation of a transaction that is billed periodically (monthly, quarterly, or annually), cancel the transaction immediately or as specified by the customer. As a service to your customers, advise the customer in writing that the service, subscription, or membership has been cancelled and state the effective date of the cancellation.

Chargeback Monitoring

As with copy requests, monitoring chargeback rates can help merchants to pinpoint problem areas in their businesses and improve prevention efforts. However, while copy request volume is often a good indicator of potential chargebacks, actual chargeback rates and monitoring strategies vary by merchant type. Card-absent merchants may experience higher chargebacks than card-present merchants as the card is not swiped, which increases liability for chargebacks.

General recommendations for chargeback monitoring include:

- **Track chargebacks and representations by reason code.** Each reason code is associated with unique risk issues and requires specific remedy and reduction strategies.
- **Include initial chargeback amounts and net chargebacks after representation.**
- **Track card-present and card-absent chargebacks separately.** If your business combines traditional retail with card-absent transactions, track the card-present and card-absent chargebacks separately. Similarly, if your business combines MO/TO and Internet sales, these chargebacks should also be monitored separately.

Visa Chargeback Monitoring Programs

Visa monitors all merchant chargeback activity on a monthly basis and alerts acquirers when any one of their merchants has excessive chargebacks.

Once notified of a merchant with excessive chargebacks, acquirers are expected to take appropriate steps to reduce the merchant's chargeback rate. Remedial action will depend on merchant type, sales volume, geographic location, and other risk factors. In some cases, you may need to provide sales staff with additional training or review sessions on card acceptance procedures. In others, you should work with your acquirer to develop a detailed chargeback-reduction plan.

Visa has three chargeback monitoring programs:



▪ **Merchant Chargeback Monitoring Program (MCMP)**

The Merchant Chargeback Monitoring Program (MCMP) monitors chargeback rates for all acquirers and merchants on a monthly basis. If a merchant meets or exceeds specified chargeback thresholds, its acquirer is notified in writing.

First notification of excessive chargebacks for a specific merchant is considered a warning. If actions are not taken within an appropriate period of time to return chargeback rates to acceptable levels, Visa may impose financial penalties on acquirers that fail to reduce excessive merchant-chargeback rates.



▪ **High-Risk Chargeback Monitoring Program (HRCMP)**

The High Risk Chargeback Monitoring Program (HRCMP) is specifically targeted at reducing excessive chargebacks by high-risk merchants. As defined by Visa, high-risk merchants include direct marketers, travel services, outbound telemarketers, inbound teleservices, and betting establishments.

HRCMP applies to all high-risk merchants that meet or exceed specified chargeback thresholds. Under HRCMP, there is no warning period and fees may be assessed to the acquirer immediately if a merchant has an excessive chargeback rate.

▪ **Global Merchant Chargeback Monitoring Program (GMCMP)**

The Global Merchant Chargeback Monitoring Program (GMCMP) is operated by Visa Inc. The program augments the U.S. Merchant Chargeback Monitoring Program (MCMP) in effect today and is intended to encourage merchants to reduce their incidence of chargebacks by using sound best practices.

The GMCMP applies when a merchant meets or exceeds specified International chargeback thresholds. Under GMCMP, there is no warning period and fees may be assessed to the acquirer immediately if a merchant has an excessive chargeback rate.

When Chargeback Rights Do Not Apply

Compliance— Another Option

Sometimes, a problem between members is not covered under Visa's chargeback rights. To help resolve these kinds of rule violations, Visa has established the compliance process, which offers members another dispute resolution option. The Visa compliance process can be used when all of the following conditions are met:

- A violation of the *Visa International Operating Regulations* has occurred.
- The violation is not covered by a specific chargeback right.
- The member incurred a financial loss as a direct result of the violation.
- The member would not have incurred the financial loss if the regulation had been followed.

Typical Compliance Violations

There are many different violations that can be classified as a compliance issue. The list below offers a quick peek at some of the compliance violations most commonly cited.

- The merchant adds a surcharge for using a Visa card as a means of payment.
- The merchant bills the cardholder for a delinquent account, or for the collection of a dishonored check.
- The merchant re-posts a charge after the card issuer initiated a chargeback.
- The merchant insists that the cardholder sign a blank sales draft before the final dollar amount is known.
- A merchant that does not hold a Visa account through an acquirer processes a transaction through another Visa merchant.

Compliance Resolution

During compliance, the filing member must give the opposing member an opportunity to resolve the issue. This is referred to as pre-compliance. If the dispute remains unresolved, Visa will review the information presented and determine which member has final responsibility for the transaction.

Section 4 Chargeback Reason Codes

The chargebacks discussed in this section are listed in numerical order.

What's Covered

- Reason Code 30: Services Not Provided or Merchandise Not Received
- Reason Code 41: Cancelled Recurring Transaction
- Reason Code 53: Not as Described or Defective Merchandise
- Reason Code 57: Fraudulent Multiple Transactions
- Reason Code 60: Illegible Fulfillment
- Reason Code 62: Counterfeit Transaction
- Reason Code 71: Declined Authorization
- Reason Code 72: No Authorization
- Reason Code 73: Expired Card
- Reason Code 74: Late Presentment
- Reason Code 75: Transaction Not Recognized
- Reason Code 76: Incorrect Currency or Transaction Code or Domestic Transaction Processing Violation
- Reason Code 77: Non-Matching Account Number
- Reason Code 80: Incorrect Transaction Amount or Account Number
- Reason Code 81: Fraud—Card-Present Environment
- Reason Code 82: Duplicate Processing
- Reason Code 83: Fraud—Card-Absent Environment
- Reason Code 85: Credit Not Processed
- Reason Code 86: Paid by Other Means
- Reason Code 96: Transaction Exceeds Limited Amount

How to Use This Information

In this section, each chargeback reason code includes the following information:

- **Definition.** Each chargeback is defined. The definition will help you understand what happened from the card issuer’s perspective; that is, what conditions or circumstances existed that caused the card issuer to issue a chargeback on the item.
- **Most Common Causes.** This section looks at the chargeback from the merchant’s perspective; that is, what may or may not have been done that ultimately resulted in the item being charged back. The “Causes” sections are short and may be helpful to you as quick references and/or for training purposes.
- **Merchant Actions.** This section outlines specific steps that merchants can take to help their acquirers remedy the chargeback, prevent future recurrence, and address customer service issues. You will also be advised under what circumstances—that is, circumstances where there is no remedy available—you should accept financial liability for the charged back item. Merchant actions are further classified by the staff functions within your establishment most likely to be responsible for taking the actions.
 - **Back-Office Staff.** The employees responsible for your general operations, administration, and processing of chargebacks and copy requests.
 - **Point-of-Sale Staff.** The employees responsible for accepting payment from customers for goods and services at the point of sale. For card-absent environments, point-of-sale staff refers to order desk staff who receive and process orders.
 - **Owner/Manager.** The employee(s) responsible for the policies, procedures, and general management of your establishment. Owners and managers may also be responsible for training.

The suggestions and recommendations for merchant actions are further classified by action type.

- **(PR) Possible Remedy.** Steps you could take to help your acquirer re-present (resubmit) a chargeback item.
- **(NR) No Remedy.** You must accept the chargeback.
- **(PM) Preventive Measures.** Possible steps you could take to minimize future recurrence of the particular type of chargeback being discussed.
- **(CS) Customer Service.** Suggestions that may help you provide enhanced service to your customers.

Disclaimer

The chargeback information in this section is current as of the date of printing. However, chargeback procedures are frequently updated and changed. Your merchant agreement and *Visa International Operating Regulations* take precedence over this manual or any updates to its information. For a copy of the *Visa International Operating Regulations* visit www.visa.com/merchant.

An overview of the chargeback life cycle and merchant responsibilities for representment and prevention can be found in *Section 1: Getting Down to Basics*.

Reason Code 30: Services Not Provided or Merchandise Not Received

Definition

The card issuer received a claim from a cardholder that merchandise or services ordered were not received or that the cardholder cancelled the order as the result of not receiving the merchandise or services by the expected delivery date (or merchandise was unavailable for pick-up).

Most Common Causes

The merchant:

- Did not provide the services.
- Did not send the merchandise.
- Billed for the transaction before shipping the merchandise.
- Did not send the merchandise by the agreed-upon delivery date.
- Did not make merchandise available for pick-up.

Merchant Actions

Back-Office Staff

Merchandise Was Delivered

(PR) If the merchandise was delivered by the agreed-upon delivery date, contact your acquirer with details of the delivery or send your acquirer evidence of the delivery, such as a delivery receipt signed by the cardholder or a carrier's confirmation that the merchandise was delivered to the correct address. If the merchandise was software that was downloaded via the Internet, provide evidence to your acquirer that the software was downloaded to or received by the cardholder.

Less Than 15 Days Since Transaction and No Delivery Date Set

(PR) If no delivery date has been specified, and the card issuer charged back the transaction less than 15 days from the transaction date, send a copy of the sales receipt to your acquirer pointing out that 15 days have not yet elapsed. You should also state the expected delivery date.

Specified Delivery Date Has Not Yet Passed

(PR) If the specified delivery date has not yet passed, return the chargeback to your acquirer with a copy of the documentation showing the expected delivery date. In general, you should not deposit sales receipts until merchandise has been shipped. For custom-made merchandise, you may deposit the entire transaction amount before shipping, provided you notify the cardholder at the time of the transaction.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 30: Services Not Provided or Merchandise Not Received

Merchandise Shipped After Specified Delivery Date

(PR) If the merchandise was shipped after the specified delivery date, provide your acquirer with the shipment date and expected arrival date, or proof of delivery and acceptance by the cardholder.

Services Were Rendered

(PR) If the contracted services were rendered, provide your acquirer with the date the services were completed and any evidence indicating that the customer acknowledged receipt.

Merchandise Was Available for Pick-Up

(PR) If you received a chargeback for merchandise that was to be picked up by the cardholder, consider the following and provide this information to your acquirer:

1. The merchandise was available for the cardholder to pick up,
2. The chargeback was processed less than 15 days from the transaction date and no pick-up date was specified, and
3. The specified pick-up date had not yet passed as noted on any internal documentation (e.g., invoice, bill of sale).

Point-of-Sale Staff

Delayed Delivery

(PM) (CS) If delivery of merchandise is to be delayed, notify the customer in writing of the delay and the expected delivery date. As a service to your customer, give the customer the option of proceeding with the transaction or cancelling it (depending on your customer service policy).

Expected Delivery

(PM) For any transaction where delivery occurs after the sale, the expected delivery date should be clearly indicated on the sales receipt or invoice.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 30: Services Not Provided or Merchandise Not Received

Owner/Manager

Proof of Delivery/Proof of Pick-Up

(PM) If you are shipping merchandise without requesting proof of delivery, consider the costs and benefits of doing so compared to the value of the merchandise you ship. Proof of delivery or pick-up, such as certified mail or a carrier's certification that the merchandise was delivered to the correct address or picked up and signed for by the cardholder, will allow you to return the chargeback if the customer claims the merchandise was not received.

Software Downloaded via Internet

(PM) If you sell software that can be downloaded via the Internet, Visa suggests that you design your website to enable you to provide evidence to your acquirer that the software was successfully downloaded and received by the cardholder.


Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 41: Cancelled Recurring Transaction

Definition

The card issuer received a claim by a cardholder that:

- The merchant was notified to cancel the recurring transaction or that the cardholder's account was closed but has since billed the customer.
- 
 ▪ The transaction amount exceeds the pre-authorized dollar amount range, or the merchant was supposed to notify the cardholder prior to processing each recurring transaction, but has not done so.

Most Common Causes



The cardholder:

- Withdrew permission to charge the account.
- Cancelled payment of a membership fee.
- Cancelled the card account.

The card issuer:

- Charged back a previous recurring transaction.
- Cancelled the card account.

The merchant:

- Received notice before the transaction was processed that the cardholder's account was closed.
- 
 ▪ Exceeded the pre-authorized dollar amount range and did not notify the cardholder in writing within ten days prior to the transaction date.
- 
 ▪ Notified the cardholder in writing within ten days of processing the recurring transaction, but cardholder did not consent to the charge.

Merchant Actions

Back-Office Staff

Transaction Cancelled and Credit Issued

(PR) If the cardholder claimed to have cancelled the recurring transaction, inform your acquirer of the date that the credit was issued.

Transaction Cancelled and Credit Not Yet Processed

(NR) If a credit has not yet been processed to correct the error, accept the chargeback. Do not process a credit; the chargeback has already performed this function.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 41: Cancelled Recurring Transaction

Transaction Not Cancelled

(NR) If you do not have a record showing that the cardholder did not cancel the transaction, accept the chargeback. The cardholder does not have to supply evidence that you received the cancellation notice.

Transaction Cancelled—Services Used

(PR) If the customer claimed they were billed for the service after they cancelled, you may need to supply proof to your acquirer that the bill in question covered services used by the customer between the date of the customer's prior billing statement and the date the customer requested cancellation.

Cardholder Expressly Renews

(PR) If the customer expressly renewed their contract for services, inform your acquirer.

Final Billing

(CS) (PM) If the customer has cancelled the recurring payment transaction and there is a final payment still to be charged, contact the cardholder directly for payment.

Customer Cancellation Requests

(CS) (PM) Always respond in a timely manner to customer requests relating to renewal or cancellation of recurring transactions. Check customer logs daily for cancellation or non renewal requests; take appropriate action to comply with them in a timely manner. Send notification to the customer that his or her recurring payment account has been closed. If any amount is owed for services up to the date of cancellation, seek another form of payment if necessary.

Credit Cardholder Account

(CS) (PM) Ensure credits are processed promptly. When cancellation requests are received too late to prevent the most recent recurring charge from posting to the customer's account, process the credit and notify the cardholder.



Transaction Exceeds Pre-authorized Amount Ranges*

(PM) (PR) Flag transactions that exceed pre-authorized amount ranges; notify customers of this amount at least ten days in advance of submitting the recurring transaction billing. If the customer disputes the amount after the billing, send evidence of the notification to your acquirer.

* This provision applies to U.S. transactions only.

Merchant Actions Legend:
(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 41: Cancelled Recurring Transaction

Owner/Manager

Train Staff on Proper Procedures

(PM) Train your sales and customer service staff on the proper procedures for processing recurring transactions as these transactions are particularly susceptible to cardholder disputes.

(PM) To minimize the risk associated with all recurring transactions, merchants should participate in Visa Account Updater (VAU)* to verify that on file information, including account number and expiration date, is correct. VAU is a Visa service that allows merchants, acquirers, and card issuers to exchange electronic updates of cardholder account information.



The VAU service ensures that merchant on-file information (cardholder account number, expiration date, status, etc.) is current. VAU allows Visa merchants, acquirers, and card issuers to electronically exchange the most current cardholder account information, without transaction or service interruption.

How the Visa Account Updater (VAU) Service Works



1. The card issuer sends information to the Visa Account Updater that includes account number, card expiration date changes, and account closures.

2. The acquirer sends inquiries to Visa Account Updater for cardholder accounts that their enrolled merchants have on file.

3. Visa Account Updater sends a response to the acquirer for each inquiry, including updated information.

4. The merchant updates the billing information for the customer.

* VAU is only available in the U.S.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 53: Not as Described or Defective Merchandise

Definition

The card issuer received a notice from the cardholder stating that the goods or services were:

- Received damaged, defective, not the same as shown and/or described on-screen (for Internet transactions), as described on the transaction receipt or other documentation presented to the cardholder at the time of the transaction.



- Not the same as the merchant's verbal description (for a telephone transaction).



- Unsuitable for the purpose in which it was sold.



For this reason code, the cardholder must have made a valid attempt to resolve the dispute or return the merchandise. An example of a valid attempt to return may be to request that the merchant retrieve the goods at the merchant's own expense.

Most Common Causes

The merchant:

- Sent the wrong merchandise to the cardholder.
- Sent the merchandise, but it was damaged during shipment.
- Inaccurately described the merchandise or services.
- Did not cancel the services purchased by the cardholder.
- Did not perform the services as described.
- Did not accept the returned merchandise.
- Accepted the returned merchandise, but did not credit the cardholder's account.

Merchants should keep in mind that their return policy has no bearing on disputes that fall under Reason Code 53: Not as Described or Defective Merchandise.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 53: Not as Described or Defective Merchandise

Merchant
Actions*Back-Office Staff***Credit Was Processed**

(PR) If merchandise was returned or services were cancelled and a credit was processed to the cardholder's account, provide your acquirer with information or evidence of the credit.

Returned Merchandise Not Received/Services Not Cancelled

(PR) If you have not received the returned merchandise (double check your incoming shipment records to verify) or the cardholder has not cancelled the service, advise your acquirer. (For U.S. transactions, the cardholder must make a valid attempt to return merchandise or cancel the service. For International transactions the cardholder must return the merchandise or cancel the service).

**Returned Merchandise Received—Credit Not Processed**

(NR) If the cardholder's complaint is valid and you received the returned merchandise but have not yet credited the cardholder's account, accept the chargeback. Do not process a credit; the chargeback has performed this function.

Merchandise Was As Described

(PR) If the merchandise was as described, provide your acquirer with specific information and invoices to refute the cardholder's claims.

Merchandise Returned Because Damaged

(PR) If merchandise was returned because it was damaged, provide evidence that it was repaired or replaced (provided the cardholder requested replacement or repair).

Services Cancelled—Credit Not Processed

(NR) If the cardholder cancelled the service but you have not yet credited the cardholder's account, accept the chargeback. Do not process a credit; the chargeback has already performed this function.

Service Performed Was As Described

(PR) If the service performed was as described or performed before the cardholder cancelled, provide your acquirer with as much specific information and documentation as possible refuting the cardholder's claims. It is recommended that you specifically address each and every point the cardholder makes.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 53: Not as Described or Defective Merchandise

Owner/Manager

Accurate Descriptions of Merchandise/Service

(CS) (PM) Ensure that descriptions of merchandise or services shown in catalogs, on Internet screens and sales receipts, or used in telephone order-taking scripts are accurate, complete, and not unintentionally misleading.

Correct Merchandise Shipped

(CS) (PM) Regularly review your shipping and handling processes to ensure that orders are being filled accurately.

Train Staff on Proper Procedures

(CS) (PM) Train staff on proper procedures for taking and filling orders; schedule review sessions at least annually.

For Your Information

Chargeback Amount Is Limited. The chargeback amount is limited to the amount of the merchandise returned or services cancelled. The chargeback may include shipping and handling fees for shipment of the defective merchandise; however, must not exceed the original amount of the transaction.

Card Issuer Waiting Period. If merchandise was returned, the card issuer must wait at least 15 calendar days from the date the cardholder returned the merchandise (to allow sufficient time for you to process a credit to the cardholder's account) before generating a chargeback. **Note:** The card issuer is not required to adhere to the waiting period if it will cause the card issuer to exceed their chargeback time frame.



Quality Disputes. This chargeback reason code also may be used for quality disputes (e.g., a car repair situation or quality of a hotel room).

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 57: Fraudulent Multiple Transactions

Definition

The card issuer received a claim from the cardholder, acknowledging participation in at least one transaction at the merchant outlet but disputing participation in the remaining transaction. The cardholder also states the card was in his or her possession at the time of the disputed transactions.

Most Common Causes

The merchant:

- Failed to void multiple transactions.
- Attempted to process transactions fraudulently.

Card-Absent Transactions

This chargeback does not apply to mail order, telephone order, or Internet transactions.

Merchant Actions

Back-Office Staff

Credit Processed on Disputed Transactions

(PR) If the appropriate credit has been processed to the cardholder's account on one or all of the disputed transactions, send your acquirer evidence of the credits.

Cardholder Participated in Multiple Transactions

(PR) If the cardholder did participate in more than one valid transaction, provide your acquirer with appropriate documentation, such as sales receipts, invoices, etc.

Credit Not Processed on Disputed Transactions

(NR) If appropriate credit has not yet been processed on the disputed transaction, accept the chargeback. Do not process a credit; the chargeback has already performed this function.

Owner/Manager

Investigate All Potentially Fraudulent Transactions

(PM) This type of chargeback could have serious implications for your establishment as it may indicate potential fraud occurring at the point of sale. It also may simply be the result of a mistake by point-of-sale staff. In either case, chargebacks of this nature require immediate investigation.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 60: Illegible Fulfillment

Definition

The card issuer requested and received a transaction receipt or substitute transaction receipt and the account number or amount is illegible.

Most Common Causes

- The merchant submitted a transaction or substitute sales receipt with an account number or amount that was not legible because:
- The point-of-sale printer ribbon was worn and the ink was too light.
 - The point-of-sale paper roll was nearing the end and the colored streak indicating this fact obscured transaction information.
 - The copy was on colored paper.
 - The carbonless paper of the original sales receipt was mishandled, causing black blotches that made copies illegible.
 - The original sales receipt was microfilmed at a reduced size, resulting in blurred and illegible copies.

Merchant Actions

Back-Office Staff

Legible or Complete Copy

(PR) If possible, resubmit a legible or complete copy of the sales receipt to your acquirer.

Incomplete Sales Receipt

(NR) If a legible copy of the sales receipt cannot be provided, accept the chargeback. (See *Section 3: Chargebacks* in this manual for further details regarding legible receipts.)

Microfilming Sales Receipts

(PM) If your establishment microfilms sales receipts, make copies from the microfilm at the same size as the original receipt. Reduced images result in blurred and illegible copies.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 60: Illegible Fulfillment

Point-of-Sale Staff

Change Point-of-Sale Printer Ribbon

(PM) Change point-of-sale printer ribbon routinely. Faded, barely visible ink on sales receipts is the leading cause of illegible receipt copies.

Change Point-of-Sale Printer Paper

(PM) The colored streak down the center or the edges of printer paper indicates the end of the paper roll. Change point-of-sale printer paper when colored streak first appears. It also diminishes the legibility of transaction information.

Keep White Copy of Sales Receipt

(PM) Keep the white copy of the sales receipt and give customers the colored copy. Colored paper does not copy as clearly as white paper and often results in illegible copies.

Carbonless Paper Used for Sales Receipts

(PM) Handle carbonless paper and carbon paper carefully. Any pressure on carbonless and carbon-back paper during handling and storage causes black blotches, making copies illegible. Always keep the top copy.

Owner/Manager

Company Logo Position on Sales Receipts

(PM) Position your company logo or marketing messages on sales receipts away from transaction information. If your company name, logo, or marketing message is printed across the face of sales receipts, the transaction information on a copy may be illegible.

(PM) For fraud-related retrieval requests, provide a copy of the signed sales receipt. However, merchants are not required to respond to retrieval requests on chip-read and PIN processed transactions.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 62: Counterfeit Transaction

Definition

The card issuer received a complaint from the cardholder claiming:

- He or she did not authorize or participate in the transaction.

Most Common Causes

Counterfeit card was used for a magnetic stripe or chip-initiated transaction that received authorization and the merchant:

- Failed to compare the first four-digits of the embossed account number on the card with the preprinted digits below the embossed number for a card-present transaction.
- Received authorization without transmission of required data.
- Accepted a chip card* containing a Visa or Visa Electron Smart Payment Application or an EMV and VIS-Compliant Plus application, but processed the chip card as a fallback transaction—via magnetic stripe, key-entry, or paper voucher, and did not follow correct acceptance procedures.

Merchant Actions

Back-Office Staff

Card and Transaction Were Valid

(PR) If the card was swiped and transaction was authorized at the point-of-sale, provide your acquirer with a copy of the printed sales receipt.

Transaction Was Counterfeit

(NR) If the transaction was counterfeit, accept the chargeback.

* A chargeback for Reason Code 62 is valid if a counterfeit copy of a chip card is used at a magnetic-stripe device (Effective October 2010).

<p>Merchant Actions Legend: (PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion</p>

Reason Code 62: Counterfeit Transaction

Point-of-Sale Staff

Check Card Security Features

(PM) Check all card security features before completing the transaction. In particular, the first four digits of the embossed account number on the card should match the printed four-digit number below the embossed number. If the numbers do not match, make a Code 10 call. You should also check to make sure that the embossed account number on the front of the card is the same as the number that appears on the terminal after you swipe the card. In addition, be sure to look for other signs of counterfeit such as embossed numbers that are blurry or uneven, or ghost images beneath the embossed numbers, indicating they have been changed.

Code 10 Calls

(PM) If you are suspicious of a card or cardholder for any reason, make a Code 10 call.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 71: Declined Authorization

Definition

The card issuer received a transaction for which authorization had been declined.

Most Common Causes

The merchant or service establishment attempted to circumvent or override a declined authorization using one of the following methods:

- **Forced posting.** After a decline or card pickup response, the merchant forced the transaction through without attempting another authorization request.
- **Multiple authorization attempts.** After an initial authorization decline, the merchant re-swiped the card one or more times until the transaction was authorized. In this situation, authorization might occur if the card issuer's authorization system times out or becomes unavailable, and the transaction is forwarded to Visa.
- **Alternative authorization method.** The merchant swiped or dipped the card at a point-of-sale terminal, and the authorization was declined. The merchant then resubmitted the transaction by key entry or called in a voice authorization and received an approval.

Merchant Actions

Back-Office Staff

Transaction Was Authorized

(PR) If you obtained an authorization approval code, inform your acquirer of the transaction date and amount.

Most acquirers will verify that an authorization approval was obtained. If the transaction was authorized, Visa systems may reject this type of chargeback as invalid so you never see it.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 71: Declined Authorization

Point-of-Sale Staff

Obtain Authorization

(PM) Obtain an authorization before completing transactions. With most point-of-sale terminals, an authorization request is sent automatically when the card is swiped or dipped and the dollar amount entered. If your terminal also has a printer, a receipt is printed if the transaction is approved and not printed if the transaction is declined.

Alternatives if Terminal Cannot Read Chip Card

(PM) If the terminal is unable to read a chip card, you can attempt to swipe or key-enter the transaction given that proper fallback indicators are provided to the issuer for approval.

Owner/Manager

Staff Awareness of Authorization Policy

(PM) Ensure that all sales staff knows your establishment's authorization policy. Inform staff that in the event of a declined transaction, they should immediately stop the transaction and ask the customer for another Visa card or other form of payment.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 72: No Authorization

Definition

The card issuer received a transaction for which authorization was not obtained or authorization was obtained using invalid or incorrect transaction data. For Automated Fuel Dispenser (AFD) transactions, the card issuer may only chargeback the amount exceeding one of the following:

- Amount authorized by the issuer
- For an EMV PIN transaction, US \$100, or local currency equivalent, if a Status Check Authorization was obtained
- For all other transactions, US \$75 or local currency equivalent, if a Status Check Authorization was obtained
- For a U.S. Domestic Visa Fleet Card transaction, US \$150, if a Status Check Authorization was obtained



Most Common Causes

- The merchant did not obtain an authorization for a transaction or, for card-present transactions, obtained it after the transaction date.
- The merchant did not exclude the tip in the authorization amount. The merchant should request an authorization for the known amount, not the transaction amount plus estimated tip.



Taxicab, limousine, bar, tavern, beauty/barber shop, health/beauty spa, and restaurant authorizations are automatically valid for the transaction amount plus 20 percent to protect merchants from chargeback liability for a disputed transaction amount.

Restaurants are permitted and protected from chargeback if they clear for an amount up to 20 percent more than they authorized, and the same is true up to 15 percent additional for T&E merchants.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 72: No Authorization

Merchant Actions

Back-Office Staff

Transaction Was Authorized

(PR) If you obtained an authorization approval, inform your acquirer of the transaction date and amount.

Transaction Was Not Authorized

(NR) Accept the chargeback.

Most acquirers will verify that a transaction was authorized and approved. If the transaction was authorized, Visa systems may reject the chargeback as invalid, and you will never see it.

Point-of-Sale Staff

Obtain an Authorization

(PM) Obtain an authorization before completing transactions. The authorization request is sent automatically when you swipe the card through a magnetic card reader or insert the card into a chip-reading device*, then enter the dollar amount. A receipt is printed if the transaction is approved; if it is not approved, you will receive a "Decline" (or "Call Center" or "Pick-Up") message on your point-of-sale terminal.

(PM) Make sure the authorization amount is equal to the check amount. Do not include the tip in your authorization request. For example, if the check before tip is US \$37.42, the authorization should be for US \$37.42.

Point-of-Sale Terminal Programming

(PM) Find out from your point-of-sale provider if your authorization system has been properly programmed to authorize only for the check amount before the tip is added.

Magnetic-Stripe Reader Down or Card's Magnetic Stripe Damaged

(PM) If you are unable to get an electronic authorization because your terminal isn't working or because the card's magnetic stripe cannot be read, you can request an authorization either by key-entering the transaction or calling your voice authorization center. If the transaction is approved, be sure the approval code is on the sales receipt in the appropriate space; in the case of a voice authorization, you will need to write it on the receipt. You should also imprint the embossed account information from the front of the card on a sales receipt or manual sales receipt form, which the customer should sign.

* Many Visa cards have a chip that communicates information to a point-of-sale terminal. If a chip-reading device is available, preference must always be given to chip card processing before attempting to swipe the stripe. The card should remain in the terminal until the transaction is complete.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 72: No Authorization

Terminal Cannot Read the Chip

(PM) If the chip-reading device cannot read the chip on the card, it means the card and chip-reading device have no applications in common. In this case, you should follow “fallback” requirements and accept the chip card via standard magnetic stripe transaction processing as prompted on the terminal screen.



Fallback refers to the action taken by a merchant to allow chip cards to be processed via magnetic stripe or key entry at chip-enabled terminals **if** the terminal fails to read the chip. Because the fallback transaction is swiped or keyed, the normal rules of transaction processing will come into play meaning that a signature will be required, rather than a PIN. In addition, manual imprints will be required for key-entered transactions. Merchants should not force a fallback transaction. Merchants are more likely to see declines for fallback transactions, than for a valid chip card transaction.

Card-Absent Transactions

Floor Limits

(PM) Floor limits are zero for all card-absent transactions with the exception of prestigious lodging merchants. This means they always require authorization regardless of the dollar amount of the transaction.

Owner/Manager

Staff Awareness of Authorization Policy

(PM) Ensure that all sales staff know your authorization policy.

Staff Training

(PM) Instruct staff to authorize only for the check amount. Emphasize that the authorization amount should equal the check amount and exclude any tip percentage.

(PM) Make sure your staff is properly trained in chip-capable terminal operation and fallback transaction processing.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 73: Expired Card

Definition	The card issuer received a transaction that was completed with an expired card and was not authorized.
Most Common Causes	The merchant accepted a card after its expiration or “Good Thru” date and did not obtain an authorization approval from the card issuer.
Merchant Actions	<p><i>Back-Office Staff</i></p> <p>Card Not Expired—Key-Entered Transaction</p> <p>(PR) For key-entered transactions, the expiration date should be on the manually imprinted copy of the front of the card. If the expiration date on the sales receipt shows the card had not expired at the time of the sale, send a copy of the receipt to your acquirer. The chargeback is invalid regardless of whether authorization was obtained.</p> <p>Card Expired, Authorization Obtained</p> <p>(PR) If the card was swiped or a manual imprint made, and authorization approval was obtained as required, inform your acquirer of the transaction date and amount. Many acquirers automatically handle this type of chargeback so you never see it.</p> <p>Card Expired, No Authorization Obtained</p> <p>(NR) If the card has expired and you did not obtain an authorization, accept the chargeback.</p> <p><i>Point-of-Sale Staff</i></p> <p>Check Expiration Date</p> <p>(PM) Check the expiration or “Good Thru” date on all cards. A card is valid through the last day of the month shown, (e.g., if the Good Thru date is 03/12, the card is valid through March 31, 2012 and expires on April 1, 2012.)</p> <p>Card-Absent, Authorization Obtained</p> <p>(PR) If the transaction was a MO/TO or Internet transaction, and authorization approval was obtained/required, inform your acquirer of the transaction amount and date. Many acquirers automatically handle this type of chargeback, so you really never see it.</p>

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 73: Expired Card

Owner/Manager

Check Card Expiration Date

(PM) Periodically remind point-of-sale staff to check the card's expiration date before completing transactions and to always obtain an authorization approval if the card has expired.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 74: Late Presentment

Definition

The transaction was not processed within the required time limits and the account was not in good standing on the processing date, or the transaction was processed more than 180 calendar days from the transaction date.

Most Common Causes

The merchant or service establishment did not deposit the sales receipt with its acquirer within the time frame specified in its merchant agreement.

Merchant Actions

Back-Office Staff

Sales Receipt Deposited on Time

(PR) If the sales receipt was deposited within the time frame specified by your acquirer, ask your acquirer to forward a copy of the receipt to the card issuer.

Sales Receipt Deposited Late—Account Closed

(NR) If the sales receipt was not deposited within 10 to 180 days of the transaction date and the cardholder account has been closed, the chargeback is valid.

(NR) For multi-location, centrally accumulated merchants (e.g., travel and entertainment, service stations), if the sales receipt was not deposited within 20 to 180 days of the transaction date and the cardholder account has been closed, the chargeback is valid.

Sales Receipt Older than 181 Days

(NR) If the sales receipt was deposited more than 181 days after the transaction date, accept the chargeback. (In this situation, the cardholder's account status is not a factor.)

Deposit Timing Guidelines

(PM) Deposit sales receipts with your acquirer as soon as possible, preferably on the day of the sale or within the time frame specified in your merchant agreement.

Time limits for depositing transactions are set to ensure timely processing and billing to cardholders. When you hold transactions beyond the period defined in your merchant agreement (usually one to five days), you lose money, affect customer service (cardholders expect to see transactions on their Visa statements within the same or next monthly cycle), and possibly invite a chargeback. No remedies exist for chargebacks on sales receipts deposited 181 days or longer after the transaction date.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 74: Late Presentment

Owner/Manager

Manual Deposit of Paper Sales Receipts

(PM) If you deposit paper sales receipts, ensure that your staff deposits them on a regular schedule within the time frame required by your acquirer.

Transaction Data Capture Terminals

(PM) Transaction data capture sales terminals allow you to electronically deposit your sales transactions after you have balanced them each day. If you currently process deposits manually, consider the costs and benefits of a transaction data capture system at the point of sale. Electronic cash registers are another option. They can be set up so that your transactions are automatically deposited in batches or on a real-time basis.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 75: Transaction Not Recognized

Definition

The card issuer received a complaint from a cardholder stating that the transaction appearing on the billing statement is not recognized. This reason code applies to both card-present and card-absent transactions.

Most Common Causes

The merchant store name or location reflected on the cardholder's billing statement was not correct or recognizable to the cardholder.

Merchant Actions

Back-Office Staff

Cardholder Participated in Transaction

(PR) Provide any documentation or information that would assist the cardholder in recognizing the transaction. **For example:**

- Sales receipt
- Shipping invoice or delivery receipts
- Description of merchandise or service purchased

Owner/Manager

Merchant Name

(PM) The merchant name is the single most important factor in cardholder recognition of transactions. Therefore, it is critical that the merchant name, while reflecting the merchant's "Doing Business As" (DBA) name, also be clearly recognizable to the cardholder. Work with your acquirer to ensure your merchant name, city, and state are properly identified in the clearing record.

(PM) The merchant is protected from a Reason Code 75: Transaction Not Recognized chargeback if the transaction has an Electronic Commerce Indicator (ECI) 5 (cardholder is fully authenticated) or ECI 6 (cardholder is not participating in Verified by Visa). The merchant must comply with the ECI process and procedures in order to benefit from this protection.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 76: Incorrect Currency or Transaction Code or Domestic Transaction Processing Violation

Definition

Transaction was processed with an incorrect transaction code, or an incorrect currency code, or one of the following:

- Merchant did not deposit a transaction receipt in the country where the transaction occurred
- Cardholder was not advised that Dynamic Currency Conversion (DCC) would occur
- Cardholder was refused the choice of paying in the merchant's local currency
- Merchant processed a credit refund and did not process a reversal or adjustment within 30 calendar days for a transaction receipt processed in error

Most Common Causes

- The merchant issued a credit voucher, but the transaction was posted as a sale.
- The transaction currency is different than the currency transmitted through VisaNet.
- Cardholder claims that the merchant failed to offer them a choice of paying in the merchant's local currency.

Merchant Actions

Back-Office Staff

Correct Transaction Code Was Posted

(PR) Provide your acquirer with documentation of the transaction, showing that it was posted correctly as a credit to the cardholder's account (and a debit to your account).

Credit Was Posted as a Debit

(NR) Accept the chargeback. In this case, the chargeback amount will be double the original transaction.

Point-of-Sale Staff

Use Correct Transaction Codes

(PM) When issuing a credit voucher, be sure to use the credit transaction code on your point-of-sale terminal.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 76: Incorrect Currency or Transaction Code or Domestic Transaction Processing Violation

Owner/Manager

Train Staff on Correct Use of Transaction Codes

(PM) Ensure all sales staff knows the procedures for issuing a credit voucher, including correct use of transaction codes on point-of-sale terminals.

Train Staff on DCC Service Requirements

(PM) If your outlet is actively involved in the offering of DCC to cardholders, ensure all sales staff know how to correctly offer this service. The training may be in any form including, but not limited to, paper guides, demonstrations etc. It is also essential that employees know how they can reverse a transaction.

Cardholder Education

(PM) Explain the DCC service to cardholders with confirmation that it is an optional service, before you begin the transaction. Recognize that language differences can sometimes provide a barrier. Good communication of the DCC service to cardholders could be facilitated by multi-lingual point-of-sale materials for cardholders.

Transaction Receipt

(PR) To aid confirmation of cardholder choice, a cardholder signature may be beneficial in proving that they agreed to participation in a DCC transaction. This would be in addition to the signature or PIN verification to confirm the transaction and cardholder identity. This is especially useful in environments where a cardholder is separated from the point-of-sale terminal such as in a restaurant, etc.

Point-of-Sale Terminal Programming

(PM) Implement a technical solution for offering DCC whereby the point-of-sale terminal automatically presents the correct prompts, clearly and accurately, to the cardholder or merchant staff.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 77: Non-Matching Account Number

Definition

The transaction did not receive authorization and was processed using an account number that does not match any on the card issuer's master file or an original credit was processed using an account number that does not match any on the card issuer's master file.

Most Common Causes

The merchant or service establishment:

- Incorrectly key-entered the account number.
- Incorrectly recorded the account number for a mail order or telephone order.

Merchant Actions

Back-Office Staff

Account Number Matches

(PR) If the account number on the sales receipt matches the account number cited on the chargeback, and the transaction received an authorization approval, return the chargeback to your acquirer and request that your acquirer include the authorization log for this transaction when returning it to the card issuer.

Account Number Doesn't Match

(NR) If the account number on the sales receipt does not match the correct account number cited on the chargeback, accept the chargeback, then process a new transaction with the correct account number and be sure to request an approval code.

After accepting the chargeback, the new transaction with the correct account number should be submitted within 10 days of the original transaction. Due to the chargeback cycle, in most cases, merchants will be unable to meet this time frame, which may in turn result in a second chargeback for Reason Code 74: Late Presentment.

For multi-location, centrally accumulated merchants (e.g., travel and entertainment, service stations), after accepting the chargeback, the new transaction with the correct account number should be submitted within 20 days of the original transaction.

Card-Absent Transactions

Transaction Authorized

(PR) If the account number on the sales receipt matches the account number cited on the chargeback, and the transaction was authorized as a mail order, telephone order, or Internet transaction, return the chargeback to your acquirer. Request that the acquirer include the authorization log for this transaction when returning it to the card issuer. Many acquirers handle this type of chargeback automatically, so that you never receive them.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 77: Non-Matching Account Number

Transaction Not Authorized

(NR) Accept the chargeback.

Point-of-Sale Staff

Terminal Can't Read Card's Magnetic Stripe

(PM) If you swipe a card and the terminal cannot read the card's magnetic stripe, request authorization by key-entering the account number. Be sure the key-entered account number matches the embossed account number on the card; be careful not to transpose numbers. Use a manual imprinter to imprint the embossed information from the face of the card onto the sales receipt that is signed by the cardholder.

Terminal Not Working or No Terminal

(PM) If your terminal is not working or you do not have a terminal, call your voice authorization center for authorization approval and write the authorization approval code on the sales receipt in the appropriate space. Use a manual imprinter to imprint the embossed information from the face of the card onto the sales receipt that is signed by the cardholder.

Embossed Account Number Does Not Match

(PM) Compare the account number displayed on your terminal (or electronically printed on the sales receipt) with the account number embossed on the card. If they do not match, do not complete the transaction. Call your voice authorization center and ask for a "Code 10 authorization" (See *Glossary*). The card issuer may ask you to pick up the card if you can do so safely.

Card-Absent Transactions

Recording Account Numbers

(PM) For phone orders, read the account number back to the customer to verify it.

Owner/Manager

Card Acceptance Procedures

(PM) Review card acceptance procedures with your point-of-sale staff. Staff should compare the account number embossed on the card with the account number printed on the related sales receipt or shown on the point-of-sale terminal. The two numbers must match. Do not accept the card if these numbers do not match; instruct your staff to call your voice authorization center and ask for a "Code 10 authorization". The card issuer may ask you to pick up the card if you can do so safely.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 77: Non-Matching Account Number

Card-Absent Transactions

Card Acceptance Procedures

(PM) Instruct staff on appropriate processing procedures for card-absent transactions. Authorization is required for all transactions where a card and cardholder are not present; staff should take extra care in recording account numbers on sales receipts and entering them into terminals. Staff should read the account number back to the customer when taking phone orders.

Recurring Payment

(PR) Because recurring payment transactions occur on a regular basis over time, it is possible that the cardholder's account number could be closed or could change (e.g., if a new card is issued due to a bank merger or account upgrade). If authorization is declined on a subsequent recurring payment transaction, contact the customer to obtain updated payment information.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 80: Incorrect Transaction Amount or Account Number

Definition

The transaction amount is incorrect, or an addition or transposition error was made when calculating the transaction amount, or a transaction was processed using an incorrect account number.

Most Common Causes

The merchant made a data entry error (i.e., keyed in the wrong amount or account number for that particular transaction).

Merchant Actions

Back-Office Staff

Transaction Amount or Account Number Is Same on Sales Receipt and Payment Documents

(PR) If the transaction amount or account number on the sales receipt is the same as on the clearing record deposited for payment, provide supporting documentation to your acquirer to re-present the item.

Incorrect or Non-matching Account Numbers

An incorrect account number transaction is one that has posted to the wrong cardholder's account. A non-matching account transaction cannot be posted; the account number does not exist on the card issuer's master cardholder file. (See Reason Code 77: Non-Matching Account Number on page 69.)

Invalid Adjustment

Many acquirers will handle this chargeback automatically so that you never receive them.

Transaction Amount or Account Number Differs (Is Incorrect)

(PR) If the transaction amount or account number on the sales receipt is not the same as on the clearing record, accept the chargeback. If the chargeback is due to an incorrect account number, process a new transaction using the correct one within 30 days of the original transaction date; however, do not process a credit because the chargeback has already performed this function. For incorrect-amount chargebacks, the chargeback amount will be the difference between the amount charged and the correct amount, so no further action is needed.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 80: Incorrect Transaction Amount or Account Number

Point-of-Sale Staff

Account Number Was Key-Entered

(PM) If the card was present, but the account number was key-entered (i.e., the magnetic stripe on the card could not be read, or the chip could not be read and processed), use a manual imprinter to imprint the card's embossed information on the sales receipt. Compare the keyed and imprinted account numbers to ensure the transaction was processed correctly.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 81: Fraud—Card-Present Environment

Definition

The card issuer received a sales receipt that is missing required information, indicating a potentially fraudulent transaction. Specific situations where this chargeback reason code may be used include:

- The card issuer received a sales receipt that has no imprint of the card's embossed or magnetic-stripe information or the cardholder's signature and either: the cardholder certifies that he or she neither authorized nor participated in the transaction OR the card issuer certifies that no valid card with that account number existed on the transaction date.
- A card-present transaction charged to a fictitious account number for which authorization approval was not obtained.

This chargeback is not valid for recurring payments and card-absent transactions. It is valid for card-present sales on self-serve point-of-sale terminals such as cardholder-activated gas pumps.

Most Common Causes

The merchant or service establishment:

- Did not swipe the card through a magnetic-stripe reader.
- Did not make a manual imprint of the card account information on the sales receipt for a key-entered transaction.
- Completed a card-present transaction without obtaining the cardholder's signature on the sales receipt.
- Completed a card-absent transaction, but did not identify the transaction as a MO/TO or Internet purchase.
- Accepted a chip card* containing a Visa or Visa Electron Smart Payment Application or an EMV and VIS-Compliant Plus application, but processed the chip card as a fallback transaction—via magnetic stripe, key-entry or paper voucher, and did not follow correct acceptance procedures**.



Fallback refers to the action taken by a merchant to allow chip cards to be processed via magnetic stripe or key entry at chip-enabled terminals **if** the terminal fails to read the chip. Because the fallback transaction is swiped or keyed, the normal rules of transaction processing will come into play meaning that a signature will be required, rather than a PIN. In addition, manual imprints will be required for key-entered transactions. Merchants should not force a fallback transaction. Merchants are more likely to see declines for fallback transactions, than for a valid chip card transaction.

* Many Visa cards have a chip that communicates information to a point-of-sale terminal with a chip-reading device. If a chip-reading device is available, preference must always be given to chip card processing before attempting to swipe the card.

** This provision does not apply to Asia Pacific.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 81: Fraud—Card-Present Environment

Merchants are not liable for a fallback to a magnetic-stripe transaction under Reason Code 81 if the proper fallback indicators were provided.

This reason code does not apply to a chip and EMV PIN transactions if a chip card is PIN-preferring, but chip terminal is not.

Merchant Actions

Back-Office Staff

Card Imprint from Magnetic Stripe Was Obtained

(PR) If account information was captured from the card's magnetic stripe, request that your acquirer send a copy of the authorization record to the card issuer as proof that the card's magnetic stripe was read. You should also provide a copy of the sales receipt proving that the cardholder's signature was obtained.

Card Imprint Was Manually Obtained

(PR) If the account number was manually imprinted on the sales receipt, send a copy of the sales receipt to your acquirer as documentation. The copy of the sales receipt must also contain the cardholder's signature in order to remedy the chargeback.

Card Imprint Was Not Obtained

(NR) If the account number was not obtained from either the magnetic stripe, the card chip, or manually, accept the chargeback. Card imprint requirements only apply if the terminal is not chip-enabled. If a chip card was manually keyed at a chip-enabled terminal, the transaction is considered a fallback and, if authorized by issuer, is not eligible for chargeback.

Signature Was Obtained

(PR) If the cardholder's signature was obtained on the sales receipt or a related document (e.g., an invoice with the cardholder's name, address, and the date of the transaction), send a copy of the document to your acquirer. You should also send evidence that the cardholder's card was present, specifically either a manually imprinted sales receipt or authorization record proving the magnetic stripe was read. You must be able to prove that the sales receipt and other documentation are from the same transaction. For example, if the imprint is on a separate receipt, the date, amount and authorization code for the transaction should also be written on this document at the point of sale.

Signature Was Not Obtained

(NR) If the cardholder's signature was not obtained for a card-present transaction, accept the chargeback.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 81: Fraud—Card-Present Environment

Merchants should always get a signature or PIN for card-present transactions, except when the transaction is processed under the Visa Easy Payment Service (VEPS). This program provides qualified face-to-face merchants with the ability to accept a Visa card issued in any country for purchases of US \$25 or under without requiring a cardholder signature or PIN and foregoing a receipt unless requested by the cardholder. For more information about VEPS and merchant eligibility.

Point-of-Sale Staff

Swipe Cards or Use a Manual Imprinter

(PM) Obtain a record of the card's account and expiration date information on the sales receipt by:

1. Swiping the card through a terminal to capture the account information from the card's magnetic stripe, or
2. Using a manual imprinter to obtain the card's embossed information.
If you use a manual imprinter, make sure the imprint can be positively matched with other transaction information to prove the card was present. For example, if you take an imprint on a separate receipt for a key-entered transaction, you should write the transaction date, amount, and authorization code on this document before completing the sale.

Obtain Cardholder Signature

(PM) Obtain the cardholder's signature on the sales receipt for all card-present transactions where a signature is required. Keep in mind that some chip cards are signature-based. The chip terminal will react to the instructions from the chip and will produce a signature line when appropriate. Always compare the customer's signature on the sales receipt to the signature on the back of the card. If the names are not spelled the same or the signatures look different, call your voice authorization center and ask for a "Code 10 authorization."

Owner/Manager

Remind Staff to Obtain an Electronic or Manual Imprint

(PM) Train sales staff to swipe the card through a magnetic-stripe terminal or to use a manual imprinter to imprint the embossed information from the front of the card onto a sales receipt that will be signed by the customer.

Manual Imprinter or Portable Electronic Terminal

(PM) If your business delivers merchandise or performs services at customers' homes, equip your field employees with manual imprinters or portable electronic terminals that can read the card's magnetic stripe or chip.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 81: Fraud—Card-Present Environment

Cardholder Signature

(PM) Train sales staff to:

1. Obtain the cardholder's signature on the sales receipt for all card-present transactions,
2. Compare the signature on the receipt to the signature on the back of the card (the names must be spelled the same), and
3. Accept only signed cards.

PIN-Verified

(PM) Make sure that the staff is aware that:

1. The chip card and chip-reading device work together to determine the appropriate cardholder or verification method for the transaction (either signature or PIN).
2. If the transaction has been PIN-verified, there is no need for a signature.

Investigate High Volume of Chargebacks

(PM) If you are receiving a high volume of Reason Code 81 chargebacks, investigate. It could be a sign of internal fraud. You may need to examine sales receipts related to the chargebacks to check which point-of-sale terminals and sales staff were involved in these transactions.

Train Staff to Clean Magnetic-Stripe Readers

(PM) A high volume of Reason Code 81 chargebacks may also indicate a need for additional staff training in proper card acceptance procedures or better maintenance and cleaning of the magnetic-stripe readers in your terminals. Ask your acquirer about point-of-sale training and educational materials and ReaderCleaner™ cards for cleaning magnetic-stripe readers. All are available from Visa.

Monitor Fallback Transaction Volume

(PM) If your business is experiencing a high volume of fallback transactions (either swiped or keyed), this may be an indication that the chip terminal has not been properly enabled. Your acquirer will be advised by Visa and should take action to remedy the situation.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 82: Duplicate Processing

Definition A single transaction was processed more than once.

Most Common Causes The merchant or service establishment:

- Entered the same transaction into the point-of-sale terminal more than once.
- Electronically submitted the same batch of transactions to its acquirer more than once.
- Deposited with its acquirer both the merchant copy and the acquirer copy of a sales receipt.
- Deposited sales receipts for the same transaction with more than one acquirer.
- Created two sales receipts for the same purchase.

Merchant Actions

Back-Office Staff

Sales Receipts Are Not Duplicates

(PR) Provide your acquirer with information documenting that the two transactions are separate, or send legible photocopies of the alleged duplicate sales receipts and any other related documents such as cash register receipts, to your acquirer. The receipts should clearly indicate that the two transactions are not charges for the same items or services.

Sales Receipts Are Duplicates—Credit Not Processed

(NR) If you have not already deposited a credit to correct the duplicate, accept the chargeback. Do not process a credit now as the chargeback has performed that function.

Sales Receipts Are Duplicates—Credit Was Processed

(PR) If you identified the duplicate transaction and processed an offsetting credit before you received the chargeback, inform your acquirer of the date the credit was issued. If your acquirer requires other procedures, follow them. However, many acquirers automatically look to see if a credit has been processed, so you may never see these chargebacks.

Review Sales Receipts Before Depositing

(PM) Review each batch of paper sales receipts prior to deposit to ensure that only acquirer copies—and not merchant copies—are included. If transactions are sent electronically for processing, ensure each batch is sent only once and has a separate batch number.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 82: Duplicate Processing

Point-of-Sale Staff

Enter Transactions Once

(PM) Take care to avoid entering the same transaction more than once.

Void Erroneous Sales Receipts

(PM) If a transaction is entered twice by mistake, void the duplicate. Any sales receipt that contains errors should be voided.

Owner/Manager

Train Sales Staff

(PM) Provide training for new point-of-sale employees (as well as refresher training for existing staff) concerning duplicate processing and related transaction reversal, cancellation, and voiding procedures. Review these procedures with sales staff whenever a mistake has been made. If duplicate transactions occur frequently, pull questionable sales receipts and related chargebacks and discuss them with the staff involved. This type of review may indicate more training is needed.

Train Staff to Void Erroneous Sales Receipts

(PM) Train point-of-sale staff to void all sales receipts that have been erroneously completed.

Correct Transaction Deposit Procedures

(PM) Train back-office staff on correct transaction deposit procedures.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 83: Fraud—Card-Absent Environment

Definition

The card issuer received:

- A complaint from a cardholder in regard to a card-absent transaction, claiming that he or she did not authorize or participate in the transaction.
- A card-absent transaction charged to a fictitious account number for which authorization approval was not obtained.



Card-absent transactions include mail order, telephone order, Internet, pre-authorized health care transactions, recurring and advance payment transactions, and no-show fees. **Note:** The pre-authorized health care transaction provision only applies to U.S. transactions.

Most Common Causes

The merchant:

- Processed a card-absent transaction from a person who was fraudulently using an account number.

The cardholder:

- Did not recognize a card-absent transaction on his or her statement due to an unclear or confusing merchant name.
- Had his or her account number taken by fraudulent means.

Merchant Actions



Back-Office Staff

Authorization Was Obtained and AVS* or CVV2 Used**

(PR) If the transaction was a MO/TO or Internet transaction and you:

- Received an authorization approval and an exact match to the AVS query (that is, a match on the cardholder's street number and ZIP code "Y" response), and have proof that the merchandise was delivered to the AVS address, send a copy of the transaction invoice, proof of delivery and any other information pertaining to the transaction to your acquirer so it may attempt a representment.
- Verified AVS or CVV2 and the card issuer gave a "U" response, you have a representment right. Inform your acquirer.

AVS* and CVV2** are primarily fraud prevention tools. In some instances **they provide merchants with a representment right**, but do not directly prevent chargebacks. When used correctly, Verified by Visa prevents issuing banks from charging back fraudulent transactions.

* AVS is only available in the U.S. and Canada.

** In certain markets, CVV2 is required to be present for all card-absent transactions.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 83: Fraud—Card-Absent Environment

Authorization Obtained, AVS or CVV2 Not Used

(PR) If you did not use AVS and the item has been charged back to you, send a copy of the transaction invoice, signed proof of delivery and any other information you may have pertaining to it to your acquirer so it may attempt a representment.

Card-Present Transaction

(PR) If the transaction was face-to-face and the card was present, the chargeback is invalid. To prove the cardholder participated in the transaction, provide your acquirer either with a copy of the sales receipt bearing the card imprint and signature of the customer or an authorization record proving the magnetic stripe was read.

Recurring Payment

(PM) Because recurring payment transactions occur on a regular basis over time, it is possible that a cardholder's account could be closed or the account number changed (e.g., if a new card is issued due to a bank merger or account upgrade). If authorization is declined on a subsequent recurring payment transaction, contact the customer to obtain updated payment information.

Point-of-Sale Staff

Obtain Authorization for All Card-Absent Transactions

(PM) Always request authorization for mail order, telephone order, Internet, and recurring transactions, regardless of the dollar amount.

Verify Account Number with Customer

(PM) For telephone transactions, always verify (read back) the account number with the customer to avoid errors.



Liability shift rules for Verified by Visa transactions may vary by region. Please check with your acquirer for further information.

* AVS is only available in the U.S. and Canada.

** In certain markets, CVV2 is required to be present for all card-absent transactions.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 83: Fraud—Card-Absent Environment

Identify Transaction as Card-Absent

(PM) All card-absent transactions should be identified by the appropriate code for MO/TO, or Internet during both the authorization and settlement process. In most cases, this will be done automatically by your transaction-processing terminal or system, or by pressing a MO/TO indicator button. If not, be sure to write the appropriate code on the transaction receipt: “MO” for mail order; “TO” for telephone order; and “ECI” for Internet.

Owner/Manager

Risk-Management Tools



(PM) For card-absent transactions, consider using AVS*, CVV2**, and Verified by Visa to help reduce fraud. Contact your acquirer for more information on these important risk-management tools.

Identifying Card-Absent Transactions

(PM) Instruct sales staff to ensure that card-absent transaction receipts contain an appropriate code identifying them as either MO/TO or Internet purchases. If the appropriate code is not printed on the receipt by your transaction-processing system, sales staff should be instructed to write it: “MO” for mail order, “TO” for telephone order, and “ECI” for Internet. In addition, if your business is processing both card-present and card-absent transactions, ensure that your staff processes the transactions appropriately. Mislabeling a card-present transaction could unnecessarily result in increased chargebacks.

Merchant Name

(PM) The merchant name is the single most important factor in cardholder recognition of transactions. Therefore, it is critical that the merchant name, while reflecting the merchant’s DBA name, also be clearly recognizable to the cardholder. You can reduce copy requests and chargebacks by working with your acquirer to ensure your merchant name, city, and state, or phone number or Internet address are properly identified in the clearing record.

(PM) The merchant is protected from a Reason Code 83: Fraud—Card-Absent Environment chargeback if the transaction has an Electronic Commerce Indicator (ECI) 5 or 6 indicating a Verified by Visa transaction. The merchant must comply with the ECI process and procedures in order to benefit from this protection.

* AVS is only available in the U.S. and Canada.

** In certain markets, CVV2 is required to be present for all card-absent transactions.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 85: Credit Not Processed

Definition

The card issuer received a notice from a cardholder acknowledging participation in a transaction for which goods were returned or services cancelled, but:

- The cardholder has not received a written refund acknowledgement or credit voucher from the merchant.
- The credit has not appeared on the customer's Visa statement.

Most Common Causes

The merchant:

- Did not issue a credit.
- Issued the credit, but did not deposit the credit with its acquirer in time for it to appear on the cardholder's next statement.
- Did not properly disclose or did disclose but did not apply a limited return or cancellation policy at the time of the transaction.
- Did not issue a credit because the business does not accept returns (but the merchant did not properly disclose its return policy).

The cardholder:

- Did not cancel a timeshare within 14 days of the contract date or receipt date.
- Did not properly cancel a guaranteed reservation or advanced deposit transaction.

Merchant Actions

Back-Office Staff

Merchandise or Cancellation Not Received

(PR) If you never received, or accepted, returned merchandise (or a cardholder's cancellation), advise your acquirer immediately. Proof of cancellation is not required from the cardholder.

Merchandise Returned Contrary to Disclosed Policy

(PR) If the cardholder returned merchandise or cancelled services in a manner contrary to your disclosed return or cancellation policy, provide your acquirer with documentation showing that the cardholder was aware of and agreed to your policy at the time of the transaction. Specifically, the cardholder's signature must appear on a sales receipt or other document stating your return policy.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 85: Credit Not Processed

Back-of-Receipt Disclosure

If your establishment's return policy is on the back of a receipt that has been signed on the front and initialed on the back as required by Visa policy, you must provide your acquirer with copies of both sides of the receipt. If the return policy is on the back of the receipt and is not signed or initialed, you have not provided evidence of proper disclosure.

Credit Was Issued

(PR) If a customer returns merchandise or cancels services in accordance with your disclosed return or cancellation policy, and you have already issued a credit, inform your acquirer of the date that the credit was issued.

Credit Not Yet Issued

(NR) If a customer returns merchandise or cancels services in accordance with your disclosed return or cancellation policy, and if you have not already issued a credit, accept the chargeback. Do not process a credit; the chargeback has already performed this function.

Issue Credits Promptly and Properly

(PM) Ensure credits are properly issued to the same Visa account that was used for the original Visa purchase.

Issue Credits Promptly

(CS) (PM) If merchandise is returned to you or services cancelled in accordance with your disclosed return or cancellation policy, issue a credit and send the customer a letter or postcard advising that you received the merchandise or cancellation request and have issued a credit to his or her account. Visa recommends that you note that due to timing, the credit may appear on the customer's next billing statement or the one after that. Typically, it takes up to five business days to post a credit.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 85: Credit Not Processed

Card-Absent Transactions



Gift Returns

(PR) In cases where a gift recipient has returned a gift ordered by mail, telephone, or the Internet, you may provide a cash or check refund, an in-store credit receipt, or another appropriate form of credit to the gift recipient. If the cardholder claims a credit was not issued to his or her account for the gift, provide appropriate documentation or information to your acquirer showing that the credit was given to the gift recipient.

Credits for Gift Returns

For gift returns, if credit is to be processed to a charge card, the credit must be issued to the same Visa account number that was used for the original transaction.

Point-of-Sale Staff

Issuing a Credit

(CS) (PM) If a customer returns merchandise as allowed by your company's return policy, issue a credit to the same Visa account that was used for the original transaction and give the customer a copy of the credit receipt. Tell customers to retain their credit receipts until the related credit appears on their Visa statement. For gift cards,* issue a cash refund or in-store credit if the cardholder states the gift card has been discarded.



Don't Wait to Issue Credits

Issue credits in a timely manner. Neglecting to issue credits promptly generates unnecessary chargebacks and creates additional back-office expenses.

Return Policy Disclosure

(PR) Be sure your establishment's return policy is clearly disclosed on sales receipts near the customer signature line before asking the cardholder to sign. If the disclosure is not properly positioned, the cardholder's signature should also be obtained in close proximity to a disclosure printed on a related document, such as a contract, invoice, or customer agreement. If the disclosure is on the back of the receipt, the cardholder must sign the front and initial the back by the disclosure statement.

* This provision applies to U.S. transactions only.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 85: Credit Not Processed

Owner/Manager

Return Policy Disclosure—At Point of Sale

(CS) (PM) Post your return policy at the cash register so that it is clearly visible to customers. Keep in mind, however, that you are required to disclose your return policy on a sales receipt or other document that is signed by the cardholder at the time of the transaction.

Return Policy Disclosure—On Sales Receipts

(PM) Be sure your return policy is clearly disclosed on your sales receipts near the customer signature line. Customers need to know your policy before they complete a sale. On receipts produced by scroll printer terminals, the disclosure must be printed in close proximity to the signature line, typically at the bottom of the transaction receipt near the transaction amount. As previously noted, if your return policy disclosures are on the back of your store's receipts, the customer must sign the front of the receipt and initial the back of the receipt by the disclosure statement.

No-Return Policy Disclosure

(PM) If your business has a limited return policy or does not allow returns at all, the words "no returns" or similar words must be preprinted on all copies of the sales receipts near the cardholder signature line.

Card-Absent Transactions

Disclosure of Return/Refund Policy

(PM) Ensure that your establishment's return or refund policy is always clearly stated in your printed advertising materials, catalog and catalog order forms, and, for Internet merchants, on your electronic order screen. Always explain your policy to customers who place orders by phone. Be sure to include refund information with the initial transaction.

Website Disclosures

For Internet transactions, the website must communicate its refund policy to the cardholder and require the cardholder to select a "click-to-accept" or other affirmative button to acknowledge the policy. The terms and conditions of the purchase must be displayed on the same screen view as the checkout screen used to present the total purchase amount or within the sequence of website pages the cardholder accesses during the checkout process.



For U.S. transactions, the refund must be disclosed during the order process.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 85: Credit Not Processed

Obtain Customer Signature

(PM) For card-absent merchants, processing mail order/telephone order transactions describing your return policy in a catalog (or verbally on the phone) does not constitute proper disclosure unless you also obtain a customer signature indicating that disclosure was provided. Such policy descriptions may support your case for having alerted the customer to your policy, however your return/refund policy may not support that the policy was properly disclosed.

Timeshare/Hotel Cancellations

(PM) For timeshare or hotel merchants it is important to provide proof that cardholder did not cancel the timeshare within 14 days, provide proof the cardholder did not cancel a guaranteed reservation, or provide proof the cancellation code provided is invalid.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 86: Paid by Other Means

Definition The card issuer received a complaint from the cardholder stating that he or she paid for the transaction by other means (i.e., cash, check, or other type of card).

Most Common Causes The cardholder initially tendered a Visa card in payment for the transaction, but then decided to use cash or a check after a credit card receipt had been completed. The merchant erroneously deposited the credit-card sales receipt in addition to the cash, check, or other payment method.

Merchant Actions

Back-Office Staff

Visa Card Was the Only Form of Payment Tendered

(PR) If a Visa card was the only form of payment tendered for the transaction, provide your acquirer with sales records or other documentation showing that no other form of payment was used.

Other Form of Payment Tendered—Credit Issued

(PR) If a Visa card sales receipt was erroneously deposited after another form of payment was used, and a credit was issued, provide your acquirer with the date of the credit. Many acquirers automatically search for credits, so you may not see these.

Other Form of Payment Tendered—Credit Not Issued

(NR) If a Visa card sales receipt was erroneously deposited after another form of payment was used, and a credit was not issued, accept the chargeback. Do not process a credit as the chargeback has already performed this function.

Point-of-Sale Staff

When Other Form of Payment Is Used, Void Visa Sales Receipt

(PM) If a customer decides to use another form of payment after you have completed a Visa card sales receipt for a transaction, make sure you void the Visa receipt and do not deposit it.

Owner/Manager

Train Staff to Void Erroneous Sales Receipts

(PM) Train sales staff in proper procedures for processing transactions where a customer decides to use another form of payment after initially offering a Visa card. Specifically, staff should be instructed to void the Visa card sales receipt and ensure that it is not deposited.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 96: Transaction Exceeds Limited Amount

Definition

The card issuer received a transaction that exceeded the allowable amount from a Limited-Amount Terminal, a Self-Service Terminal, or an Automated Fuel Dispenser (AFD) transaction.

Most Common Causes



For U.S., the merchant processed a transaction from:

- A Limited-Amount Terminal and Exceeded US \$25
- A Self-Service Terminal (excluding AFD) and Exceeded US \$50
- An AFD and Exceeded:
 - US \$150 for Visa Fleet cards
 - US \$75 for all other cards
 - US \$500 for a Real-Time Clearing transaction



For International, the merchant processed a transaction in excess of permitted amounts from:

- A Cardholder-Activated Transaction Type A
- A Cardholder-Activated transaction Type B
- A Real Time Clearing (RTC) transaction

Merchant Actions

Back-Office Staff

Transaction Was Less Than the Allowable Amount of US \$25, US \$50, or Amounts Specified for AFD

(PR) – Provide documentation to the acquirer supporting the transaction amount (e.g., copy of the sales receipt or audit tape).

Transaction Amount Exceeded US \$25, US \$50, or Amounts Specified for AFD

(NR) – Accept the chargeback. Transaction exceeded allowable limit for a Limited-Amount Terminal, a Self-Service Terminal, or an AFD.

Credit Processed on Disputed Transaction

(PR) – If the appropriate credit has been processed to the cardholder's account on the disputed transaction, send your acquirer evidence of the credit.

Reason Code 96: Transaction Exceeds Limited Amount

Credit Not Processed on Disputed Transaction — Transaction Exceeded Allowable Amount

(NR) – If the appropriate credit has not yet been processed on the disputed transaction, accept the chargeback. Do not process a credit since the chargeback has already performed this function.

Note: For AFD transactions, the amount of the card issuers' chargeback is limited to the amount exceeding the specified amounts noted above.

Chargeback Was Invalid

(PR) – If the transaction was not conducted at an unattended terminal (i.e., Limited-Amount, Self-Service, or AFD) provide proof to the acquirer.

Example:

The card issuer claims the transaction exceeded the allowable amount for an AFD (Merchant Category Code 5542) transaction and processed a chargeback. The original transaction amount was US \$85; the card issuer processed a chargeback for US \$10, which represents the amount that exceeded the allowable amount. The merchant's audit records show the transaction was completed inside the convenience store (Merchant Category Code 5541). The merchant provides evidence to its acquirer. In this example, the card issuer's chargeback would be considered invalid if the merchant can provide a sales receipt with the cardholder's signature and card imprint.

Note: To avoid chargebacks, ask your acquirer to verify that your AFD and convenience store terminals are accurately programmed with the correct Merchant Category Codes. All AFD terminals should have a Merchant Category Code of 5542 and your inside store location should have Merchant Category Code of 5541.

Owner/Manager

Transaction Was Above US \$25, US \$50, or Amount Specified for AFD

(PM) Evaluate potential risk of chargeback exposure by ensuring terminals are properly set at transaction amount limits.

Example:

If you are an AFD merchant, consider limiting fuel distribution to Visa's allowable amount. Complying with Visa's allowable limits will reduce your exposure to this chargeback reason code.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Appendix 1: Training Your Staff

Training is Good Business

Cardholders expect and depend on accurate, efficient card processing when shopping with a Visa merchant.

Your sales staff and customer service associates play a critical role in ensuring proper transaction processing. Ensuring that they receive regular and ongoing training in Visa card acceptance policies and procedures benefits everybody.

- Sales staff and customer service associates benefit because they are given the skills and knowledge they need to do their jobs accurately and confidently.
- You benefit because:
 - Customer service is enhanced, leading to increased sales.
 - You may have fewer fraudulent transactions, which reduces related losses.
 - You may have fewer transaction receipt copy requests and chargebacks, which reduces related expenses.

It is important that your sales staff and customer service associates understand the proper card acceptance procedures, which are easy to learn and can help you. Visa resources are available at your Visa.com regional site. Please visit www.visa.com for the latest products and services for Visa merchants. No matter how much experience your employees have, you will find these materials very useful for teaching your staff.



Your customers will have used their cards with many different retailers and will expect their transactions to be processed in the same basic way at your business. By serving them quickly and efficiently they will have fewer reasons to complain or to dispute a transaction. Satisfied customers tend to remain loyal to your business, and return more often.





Card Acceptance Guidelines for Visa Merchants

The *Card Acceptance Guidelines for Visa Merchants* is a comprehensive manual for all businesses that accept Visa transactions in the card-present and/ or card-absent environment. The purpose of this guide is to provide merchants and their back-office sales staff with accurate, up-to-date information and best practices to help merchants process Visa transactions, understand Visa products and rules, and protect cardholder data while minimizing the risk of loss from fraud.

For a copy of this document, contact your acquirer.

Appendix 2: Glossary


Account number	The 16-digit account number that appears in print on the front of all valid Visa cards. The number is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid.
Acquirer	A financial institution that enters into agreements with merchants to accept Visa cards as payment for goods and services. Also called acquirers or acquiring banks.
Address Verification Service (AVS)	AVS* allows merchants that accept card-absent transactions to compare the billing address (the address to which the card issuer sends its monthly statement for that account) given by a customer with the billing address on the card issuer's master file before shipping an order. AVS helps merchants minimize the risk of accepting fraudulent transactions in a card-absent environment by indicating the result of the address comparison.
	 
ATM	An unattended magnetic-stripe or chip-reading terminal that has electronic capability, accepts PINs, and disburses currency or travelers cheques.
Authorization	The process by which a card issuer approves or declines a Visa card purchase. Authorization occurs automatically when you swipe the magnetic stripe of a payment card through a card reader. See also, <i>Voice Authorization Center</i> .
"Call" or "Call Center" response	A response to a merchant's authorization request indicating that the card issuer needs more information about the card or cardholder before a transaction can be approved. Also called a "Referral" response.
Card acceptance procedures	The procedures a merchant or merchant employee must follow at the point-of-sale to ensure that a card and cardholder are valid.
Card expiration date	See " <i>Good Thru</i> " date.
Cardholder	The person to whom a Visa card is issued.
Card issuer	A financial institution that issues Visa cards.
Card-absent	A merchant, market, or sales environment in which transactions are completed without a valid Visa card or cardholder being present. Card-absent is used to refer to mail order, telephone order, and Internet merchants and sales environments.


* AVS is only available in the U.S. and Canada.

Card-present	A merchant, market or sales environment in which transactions can be completed only if both a valid Visa card and cardholder are present. Card-present transactions include traditional retail environment (department and grocery stores, electronics stores, boutiques, etc.) cash disbursements, and self-service situations, such as gas stations and grocery stores, where cardholders use unattended payment devices.
Card security features	The alphanumeric, pictorial, and other design elements that appear on the front and back of all valid Visa credit and debit cards, as specified in the <i>Visa International Operating Regulations</i> . Card-present merchants must check these features when processing a transaction at the point-of-sale to ensure that a card is valid. Card-present merchants are not required to check security features on chip cards. In most cases, the merchant will not handle the card.
Card Verification Value (CVV)	A unique three-digit “check number” encoded on the magnetic-stripe of all valid cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe- encoded account information and is verified online at the same time a transaction is authorized.
Card Verification Value 2 (CVV2)*	A Visa fraud prevention system used in card-absent transactions to ensure that the card is valid. The CVV2 is the three-digit value that is printed on the back of all Visa cards. Card-absent merchants ask the customer for the CVV2 and submit it as part of their authorization request. For information security purposes, merchants are prohibited from storing CVV2 data.
Card Verification Value for Integrated Circuit Cards (iCVV)	An alternate CVV defined for storage on a Visa EMV chip card. It uses “999” instead of the service code encoded on the magnetic stripe image of the chip for the iCVV calculation. iCVV enables issuers to identify fraudulent use of chip data in magnetic-stripe read transaction processing.
Cash disbursement	A bankcard transaction involving the payment of cash or travelers cheques to a cardholder. In general, only financial institution branches are allowed to make cash disbursements.
Chargeback	A transaction that is returned as a financial liability to an acquirer by a card issuer, usually because of a disputed transaction. The acquirer may then return or “charge back” the transaction to the merchant. To be valid, a chargeback must be in accordance with <i>Visa International Operating Regulations</i> .
Chip	An integrated microchip that is embedded into a plastic credit or debit card. It is virtually impossible to copy, facilitates the evolution of security methods and processes, and is capable of holding many applications.
Chip card	A plastic credit card with an embedded computer chip that communicates information to a chip-reading device during the transaction process.

* In certain markets, CVV2 is required to be present for all card-absent transactions.

Chip-initiated transaction	An EMV and VIS-compliant chip card transaction which is processed at a chip-reading device using full-chip data, and limited to Visa and Visa Electron Smart Payment Applications, or EMV and VIS-compliant Plus applications.
Chip-reading device	A point-of-transaction terminal capable of reading, communicating, and processing transaction data from a chip card. The chip card and chip-reading device work together to determine the appropriate cardholder or verification method for transaction (either signature or PIN).
Code 10 call	A call made by a sales associate to the merchant's voice authorization center when the appearance of a card or the actions of a cardholder suggest the possibility of fraud. The term "Code 10" is used so calls can be made without arousing suspicion while the cardholder is present. Specially trained operators then provide assistance to point-of-sale staff on how to handle the transaction.
Copy request	A request by a card issuer to an acquirer for a copy or facsimile of a sales receipt for a disputed transaction. Depending on where sales receipts are stored, the acquirer either fulfills the copy request itself or forwards it to the merchant for fulfillment. A copy request is also known as a retrieval request. Copy requests are no longer required for chip card, EMV PIN transactions (except in the case of T&E document requests, cash, quasi-cash, and VEPS transactions.)
Credit receipt	A receipt documenting a refund or price adjustment that a merchant has made or is making to a cardholder's account. Also called credit voucher.
CyberSource Advanced Fraud Screen Enhanced by Visa	A real-time fraud detection service that examines transactions generated from online stores. It estimates the level of risk associated with each transaction and provides merchants with risk scores, enabling them to more accurately identify potentially fraudulent orders.
Disclosure	Merchants are required to inform cardholders about their policies for merchandise returns, service cancellations, and refunds. How this information is conveyed, or disclosed, varies for card-present and card-absent merchants, but in general, disclosure must occur before a cardholder signs a receipt to complete the transaction.
Dynamic Currency Conversion (DCC) Service	An optional, non-Visa service that facilitates the conversion of the purchase price of goods or services from the currency in which the purchase price is displayed to another currency as agreed to by the cardholder and merchant. That currency becomes the transaction currency, regardless of the merchant's local currency.
Electron card	A debit or prepaid card that is issued in countries around the world. The card is currently not issued in the U.S., but is accepted at many U.S. merchant locations. Electron cards have slightly different security features than other Visa cards: the front of the card contains an Electron rather than a dove hologram, and the 16-digit account number is printed, not embossed. For this reason, the Electron card must be authorized electronically (i.e., not permitted for key-entered transactions).

Electronic Commerce Indicator (ECI)	A transaction data field used by e-commerce merchants and merchant acquirer to differentiate Internet merchants from other merchant types. Use of the ECI in authorization and settlement messages helps e-commerce merchants meet Visa processing requirements and enables Internet transactions to be distinguished from other transaction types. Visa requires all e-commerce merchants to use the ECI.
Exception file	A list of lost, stolen, counterfeit, fraudulent, or otherwise invalid account numbers kept by individual merchants or their third party processors. The exception file should be checked as part of the authorization process, particularly for transactions that are below a merchant's floor limit.
Firewall	A security tool that blocks access from the Internet to files on a merchant's or third party processor's server and is used to ensure the safety of sensitive cardholder data stored on a server.
Global Merchant Chargeback Monitoring Program (GMCMP)	Augments the U.S. Merchant Chargeback Monitoring Program (MCMP) in effect today and is intended to encourage merchants to reduce their incidence of chargebacks by using sound best practices. The GMCMP applies when a merchant meets or exceeds specified International chargeback thresholds. Under GMCMP, there is no warning period and fees may be assessed to the acquirer immediately if a merchant has an excessive chargeback rate.
"Good Thru" date	The date after which a bankcard is no longer valid; it is embossed on the front of all valid Visa cards. The Good Thru date is one of the card security features that should be checked by merchants to ensure that a card-present and card-absent transaction is valid. See also, <i>Card expiration date</i> .
High-Risk Chargeback Monitoring Program (HRCMP) — U.S. Only	Applies to all high-risk merchants that meet or exceed specified chargeback thresholds. Under HRCMP, there is no warning period and fees may be assessed to the acquirer immediately if a merchant has an excessive chargeback rate.
	
High-risk merchant	A merchant that is at a high risk for chargebacks due to the nature of its business. As defined by Visa, high-risk merchants include direct marketers, travel services, outbound telemarketers, inbound teleservices, and betting establishments. See also, <i>High-Risk Chargeback Monitoring Program</i> .
Internet Protocol address	A unique number that is used to represent individual computers in a network. All computers on the Internet have a unique IP address that is used to route messages to the correct destination.
Issuer	A financial institution (or other authorized entity) that issues Visa cards to cardholders.

Key-entered transaction	A transaction that is manually keyed into a point-of-sale device.
Magnetic stripe	The magnetic stripe on the back of all Visa cards is encoded with account information as specified in the <i>Visa International Operating Regulations</i> . The stripe is “read” when a card is swiped through a point-of-sale terminal. On a valid card, the account number on the magnetic stripe matches the account number on the front of the card.
Magnetic-stripe reader	The component of a point-of-sale device that electronically reads the information on a payment card’s magnetic stripe.
Mail Order/ Telephone Order (MO/TO)	A merchant, market, or sales environment in which mail or telephone sales are the primary or major source of income. See also, <i>Card-absent</i> .
Member	An organization that is a financial institution or other entity authorized to issue cards and/or sign merchants. Also referred to as a Visa client.
Merchant agreement	The contract between a merchant and an acquirer under which the merchant participates in the Visa payment system, accepts Visa cards for payment of goods and services, and agrees to abide by certain rules governing the acceptance and processing of Visa transactions. Merchant agreements may stipulate merchant liability with regard to chargebacks and may specify time frames within which merchants are to deposit transactions and respond to requests for information.
Merchant Chargeback Monitoring Program (MCMP) — U.S. Only	A Visa program that alerts acquirers when one of their merchants has a chargeback-to-transaction rate of over one percent. Merchants then work with the acquirer to reduce their chargeback rates to acceptable levels. Failure to reduce chargebacks can result in fines for a merchant.
	
Merchant Servicer (MS)	An MS stores, processes, or transmits Visa account numbers on behalf of a member’s merchant. Function examples include providing such services as online shopping cards, gateways, hosting facilities, data storage, authorization and/or clearing and settlement messages.
Payment Card Industry Data Security Standard (PCI DSS)	A comprehensive set of international security requirements for protecting cardholder data. The PCI DSS was developed by Visa and other major card brands to help facilitate the broad adoption of consistent data security measures on a global basis.
Personal Identification Number (PIN)	A personal identification alpha or numeric code that identifies a cardholder in an authorization request originating at a terminal with electronic capability.

Pick-up response	An authorization response instructing a card-present merchant to refuse a transaction and recover the card. In all circumstances, card recovery should only be attempted if it can be done by reasonable and peaceful means.
Point-Of-Sale (POS) terminal	The electronic device used for authorizing and processing bankcard transactions at the point of sale.
Printed number	A four-digit number that is printed below the first four digits of the printed or embossed account number on all valid Visa cards. The four-digit printed number should begin with a "4," and be the same as the first four digits of the account number above it. The printed four-digit number is one of the card security features that merchants should check to ensure that a card-present transaction is valid.
Processor	A member, or Visa-approved non-member acting as the Agent of a member, that provides authorization, clearing, or settlement services for merchants and members. The <i>Visa International Operating Regulations</i> refers to the three types of processors: authorizing processors, clearing processors, and V.I.P. system users. See also, <i>VisaNet processor</i> .
Representment	A chargeback that is rejected and returned to a card issuer by an acquirer on the merchant's behalf. A chargeback may be re-presented, or redeposited, if the merchant or acquirer can remedy the problem that led to the chargeback. To be valid, a representment must be processed in accordance with <i>Visa International Operating Regulations</i> .
Sales receipt	The paper or electronic record of a bankcard transaction that a merchant submits to an acquirer for processing and payment. In most cases, paper drafts are now generated by a merchant's point-of-sale terminal. When a merchant fills out a draft manually, it must include an imprint of the front of the card.
Skimming	The replication of account information encoded on the magnetic stripe of a valid card and its subsequent use for fraudulent transactions in which a valid authorization occurs. The account information is captured from a valid card and then re-encoded on a counterfeit card. The term "skimming" is also used to refer to any situation in which electronically transmitted or stored account data is replicated and then re-encoded on counterfeit cards or used in some other way for fraudulent transactions.
Split tender	The use of two forms of payment, or legal tender, for a single purchase. For example, when buying a big-ticket item, a cardholder might pay half by cash or check and then put the other half on his or her Visa credit card. Individual merchants may set their own policies about whether or not to accept split-tender transactions.
Third Party Agents	An entity that provides payment related services, directly or indirectly, to a member and/or stores, processes, or transmits cardholder data. A Third Party Agent must be registered by all Visa members utilizing their services, directly or indirectly.

Third party processor	A non-member organization that performs transaction authorization and processing, account record keeping, and other day-to-day business and administrative functions for card issuers and acquirers.
Transaction	The act between a cardholder and a merchant that results in the sale of goods or services.
Unsigned card	A seemingly valid Visa card that has not been duly signed by the legitimate cardholder. Merchants cannot accept an unsigned card until the cardholder has signed it and the signature has been checked against valid government identification, such as a driver's license or passport.
Verified by Visa	A Visa Internet payment authentication system that validates a cardholder's ownership of an account in real-time during an online payment transaction. When the cardholder clicks "Buy" at the checkout page of a participating merchant website, a Verified by Visa screen automatically appears on the cardholder's desktop. The cardholder enters a password that allows the card issuer to verify his or her identity.
Visa Easy Payment Service (VEPS)	Provides face-to-face merchants with the ability to accept a Visa card issued in any country for purchases of US \$25 or under without requiring a cardholder signature or PIN and foregoing a receipt unless requested by the cardholder.
Visa payWave	A new payment method that sends card data wirelessly to a terminal reader. A cardholder simply holds their card in front of the reader. For many transactions, there is no need to sign a receipt or hand over the card.
VisaNet processor	A processor directly connected to VisaNet. See also, <i>Processor</i> .
Voice authorization	An authorization obtained by telephoning a voice authorization center.
Voice authorization center	An operator-staffed center that handles telephone authorization requests from merchants who do not have electronic point-of-sale terminals or whose electronic terminals are temporarily not working, or who have transactions that require special assistance. Voice authorization centers also handle manual authorization requests and Code 10 calls.

Appendix 3: Visa Europe Territory

The following is a list of European economic area's where participation in the Visa payment system is governed by the *Visa Europe Operating Regulations*, as of the date of this publication.

Andorra	Hungary
Austria	Latvia
Belgium	Liechtenstein
Cyprus	Luxembourg
Denmark	Malta
Czech Republic	Monaco
Faeroe Islands	Netherlands
Finland	Lithuania
France, Metropolitan	Norway
France	Portugal
Germany	Poland
Gibraltar	San Marino
Greece	Spain
Greenland	Svalbard & Jan Mayen Is.
Estonia	Slovakia
Vatican City State	Slovenia
Iceland	Sweden
Republic of Ireland	Switzerland
Israel	Turkey
Italy	United Kingdom

