Card Acceptance and Chargeback Management Guidelines for Visa Merchants

Card Acceptance and Chargeback Management Guidelines for Visa Merchants

Table of Contents

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Introduction

What's Covered

- Purpose and Audience
- Contents

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Purpose and Audience

For today's Visa® merchant, accepting Visa payment cards has become simultaneously easier and more complex. Electronic terminals and card acceptance devices make transaction processing automatic and seemingly effortless, raising potential profitability. However, they also create increased possibilities for processing mistakes and fraudulent transactions that can result in copy requests and chargebacks.

In addition, the walls between card-present and card-absent transactions have become less obvious as growing numbers of traditional "brick and mortar" merchants launch e-commerce websites, transforming themselves into "click and mortar" businesses. Such merchants must, in effect, be "bilingual"—familiar with both card-present and card-absent procedures.

Card Acceptance and 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 sales staffs with accurate, up-to-date information on processing Visa transactions while minimizing the risk of loss from fraud and chargebacks. This book is targeted at both card-present and card-absent merchants and their employees and includes requirements and best practices for doing business on the Internet. It also contains detailed information on the most common types of chargebacks merchants receive and what can be done to remedy or prevent them.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Contents

Card Acceptance and Chargeback Management Guidelines for Visa Merchants 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—**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: Card-Present Transactions—**Requirements and best practices for processing card-present transactions at the point of sale including how to minimize key-entered transactions and ensure legible sales receipts. Suspicious transactions, Code 10 calls, and card recovery procedures are also discussed.
- ✔ **Section 3: Card-Absent Transactions—**Requirements and best practices for processing card-absent transactions including mail order, telephone order, and Internet sales. Visa fraud prevention tools, such as the Address Verification Service and Card Verification Value 2 (CVV2); requirements for e-commerce websites; and procedures for recurring transactions are also covered.
- ✔ **Section 4: Payment Card Industry Data Security Standard and PIN Security and Key Management—**CISP is the Payment Card Industry (PCI) Data Security Standard (DSS) that Visa requires merchants and their service providers to implement to ensure the security of confidential cardholder account information.
- ✔ **Section 5: Copy Requests—**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 6: Chargebacks—**Requirements and best practices for processing transactions that are charged back to you by your merchant bank (from the card issuer). This section includes strategies for chargeback prevention, as well as information on how and when to resubmit a charged-back transaction to your merchant bank. A brief compliance process overview is also included.
- ✔ **Section 7: Chargeback Reason Codes—**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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

- ✔ **Appendix 1: Training Your Troops—**A comprehensive list of Visa print and multimedia materials 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.

Disclaimer

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

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

SECTION 1 Getting Down to Basics

What's Covered

- Visa Transaction Processing—From Start to Finish
- Visa Rules
- Visa Rules for Returns and Exchanges
- Visa Rules for PIN-less Payment Brand Acceptance
- Dynamic Currency Conversion (DCC) Compliance

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa Transaction Processing—From Start to Finish

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. This basic knowledge will provide you with a conceptual framework for the policies and procedures covered in this guide. It will also help you to understand the major components of payment processing and how they affect the way you do business.

Who Does What—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.

A merchant bank is a financial institution that contracts with merchants to accept Visa cards for payment of good and services. A merchant bank may also contract with third party processors to provide these 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 is a public corporation that works with financial institutions that issue Visa cards and/or sign merchants to accept Visa cards for payment of goods and services. Visa provides card products, promotes the Visa brand, and establishes the rules and regulations governing member participation in Visa programs. Visa also operates the world's largest retail electronic payments network to facilitate the flow of transactions between members.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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

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

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 slightly for any one merchant, merchant bank, or card issuer, depending on card and transaction type, and the processing system used.

Authorization

1. Cardholder *presents a Visa card to pay for purchases. For card-absent transactions, the cardholder provides the merchant with the account number, expiration date, billing address, and CVV2.*

2. Merchant *swipes the card, enters the dollar amount, and transmits an authorization request to the merchant bank. For card-absent transactions, the account number and other information may be digitally or key-entered.*

3. Merchant bank *electronically sends the authorization request to VisaNet.*

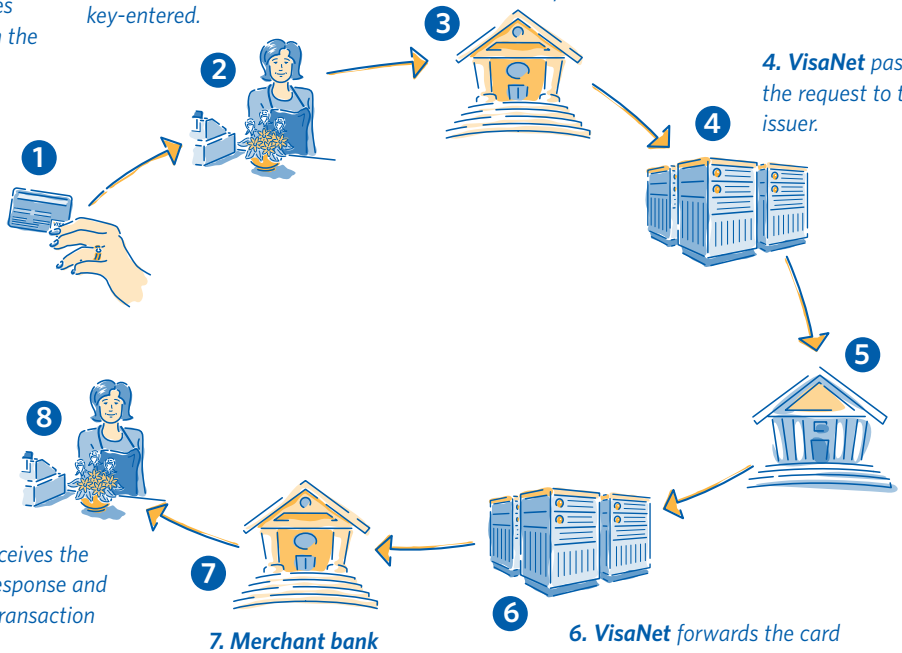
4. VisaNet *passes on the request to the card issuer.*

5. Card issuer *approves or declines the transaction.*

6. VisaNet *forwards the card issuer's authorization response to the merchant bank.*

7. Merchant bank *forwards the response to the merchant.*

8. Merchant *receives the authorization response and completes the transaction accordingly.*

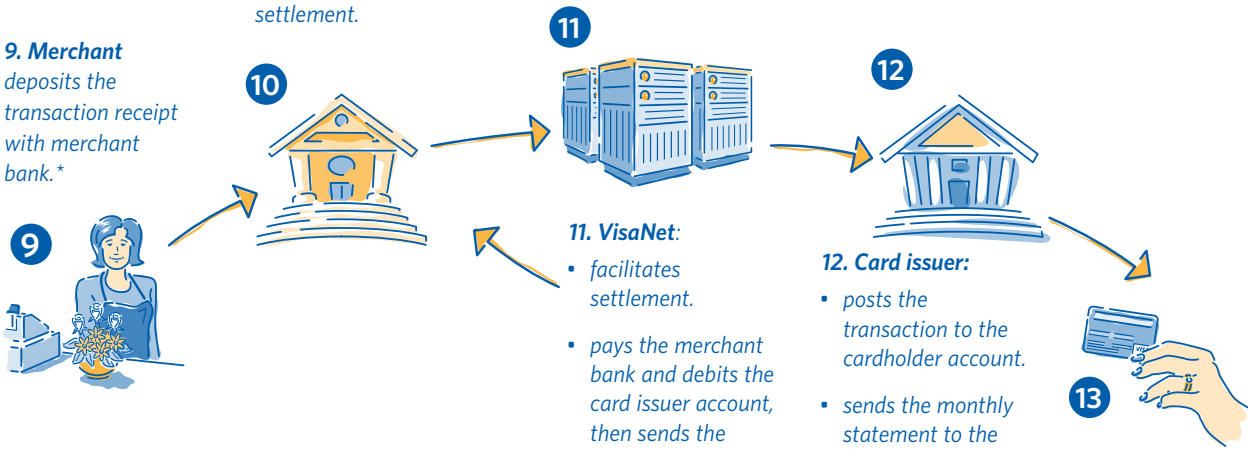


©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Clearing and Settlement

10. Merchant bank *credits the merchant's account and electronically submits the transaction to Visa for settlement.*

9. Merchant *deposits the transaction receipt with merchant bank.**



11. VisaNet*:*

- *facilitates settlement.*
- *pays the merchant bank and debits the card issuer account, then sends the transaction to the card issuer.*

12. Card issuer:

- *posts the transaction to the cardholder account.*
- *sends the monthly statement to the cardholder.*

13. Cardholder *receives the statement.*

Merchants or their agents that store, process, or transmit data may **not store sensitive authentication data (full magnetic-stripe or chip) contents. Card Verification Value 2 (CVV2), or PIN Verification Value (PVV)—even if it is encrypted. Once an authorization is processed, such data should no longer exist. The **only** components of the magnetic stripe that can be stored are the cardholder's name, account number, and expiration date.*

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa Rules

U.S. merchants must follow basic card acceptance rules for all Visa transactions. Careful and consistent adherence to the Visa USA rules outlined in this section will help you to enhance customer satisfaction and increase your profitability. If you have any questions about any of the Visa rules presented here, contact your merchant bank.

Acceptance Options

To offer the broadest possible range of payment options to consumers, most merchants choose to accept all categories of Visa debit and credit cards. U.S. merchants, however, may accept:

- All Visa cards
- Visa credit and business cards only
- Visa consumer debit and prepaid cards only

These acceptance options apply only to cards issued in the United States. Merchants accepting any category of Visa cards must honor all foreign-issued Visa cards presented for payment.

Visa Logo

Display the Visa logo at the merchant location or on catalogs, sale materials, or websites. Depending on the card acceptance option you choose, both card-present and card-absent merchants must display the appropriate Visa logo or wordmark to advise customers of your payment options. Visa has developed the following logos:

All Visa Cards accepted

Visa Debit Category accepted (Merchant chooses not to accept credit and business category)

Visa Credit and Business Category accepted (Merchant chooses not to accept debit category)

For Automated Fuel Dispensing (AFD) merchants, the Visa logo must be displayed on or near the dispenser.

Dollar Minimums and Maximums

Always honor valid Visa cards in your acceptance category, regardless of the dollar amount of the purchase. Imposing minimum or maximum purchase amounts in order to accept a Visa card transaction is a violation of the Visa rules.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

No Surcharging

Always treat Visa transactions like any other transaction; that is, you may not impose any surcharge on a Visa transaction. You may, however, offer a discount for cash or another form of payment (e.g., proprietary card or gift certificate) provided that the offer is clearly disclosed to customers and the cash price is presented as a discount from the standard price charged for all other forms of payment.

The discount may not be applied to a "comparable card." A "comparable card" is any other branded, general purpose payment card that uses the cardholder's signature as the primary means of cardholder authorization (e.g., MasterCard, Discover, American Express). Any discount made available to cardholders who pay with "comparable cards" must also be made available to cardholders who wish to pay with Visa cards.

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 the following rules:

- The fee is being charged for a bona fide convenience of using an alternative payment channel outside of the merchant's normal business practice (see example below).
- The fee:
  - must be disclosed to the customer as a charge for the alternative payment channel convenience
  - is applied only to non face-to-face transactions
  - must be a flat or fixed amount, regardless of the amount of the payment due
  - is applied to all forms of payment products accepted in the alternative payment channel
  - is included as part of the total transaction amount
  - cannot be added to a recurring transaction
  - is assessed by the merchant that provides the goods or services to the cardholder and not a third party
- The customer must be given the opportunity to cancel prior to the completion of the transaction

Example:

The merchant provides utility services to its customers, and the customary way to pay is by mail or in person at the merchant's location. For the convenience of its customers, the merchant also offers a website for payments. In this example, the merchant may apply a convenience fee to payments made via the website.

For further information on Convenience Fees, please contact your merchant bank.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Taxes

Include any required taxes in the total transaction amount. Do not collect taxes separately in cash. Among other things, this policy reflects the needs of the many Visa cardholders who must have written records of the total amount they pay for goods and services, including taxes.

Laundering

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

Zero-Percent Tip

For restaurant, taxicab, limousine, bar, tavern, beauty/barber shop, and health/beauty spa merchants 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. Consequently, 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.

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 receipts within five calendar days of the transaction date. The sooner you deposit transaction receipts with your merchant bank, the sooner you get paid. For card-absent transactions, the transaction date is the **ship date**, not the order date. Transactions deposited more than 30 days after the original transaction date may be charged back to you.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Truncation of Account Number and Expiration Date

Truncated Account Number. Visa requires that all electronic POS terminals provide account number truncation on transaction receipts. This means that only the last four digits of an account number should be printed on the customer's copy of the receipt.

The expiration date should not appear at all. Existing POS terminals must comply with these requirements. To ensure that your POS terminals are properly set up for account number and expiration date truncation, contact your merchant bank.

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 delivered.

Delayed Delivery

For a delayed delivery, obtain 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:

- **Create two transaction receipts**—one for the deposit and one for the balance. Write "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 POS device does not automatically print authorization codes on sales receipts, write the codes on the receipts so they are clearly identifiable as such.
- **Write "Delayed Delivery,"** along with the authorization code, on each transaction receipt.

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

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 merchant bank 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* on page 57.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Merchant Servicer Registration

Visa merchant banks must register Third Party Agents (TPA) who are handling Visa account numbers for their merchants, in accordance with the *Visa U.S.A. Inc. Operating Regulations*. A Merchant Servicer (MS) is defined by Visa as a TPA that has a direct relationship with a merchant and is storing, processing or transmitting Visa account numbers on the merchants behalf. This type of TPA performs services such as payment gateway, shopping cart, fraud scrubbing, loyalty programs, etc. Member banks and their merchants are responsible for ensuring MS' maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS), validate PCI DSS compliance with Visa and are correctly registered as an MS with Visa.

Merchants should work with their Visa merchant banks to ensure all TPA rules and requirements have been satisfied, ensuring the merchants compliance with *Visa U.S.A. Inc. Operating Regulations*.

Any TPA's a merchant is using should be listed on Visa's compliant service providers list. The CISP list of Compliant 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* on page 57.

Data Storage

Merchants should also be aware of the following data security requirements and best practices:

- **Minimize Cardholder Data Retention and Eliminate Magnetic Stripe Data Storage**. The *Visa U.S.A. Inc. Operating Regulations* prohibit merchants and/or their agents from storing the full contents of the magnetic stripe after transaction authorization. Storage of some data elements from the magnetic stripe is permitted, including the cardholder's name, primary account number, expiration data and service code.However, these values should only be stored if needed to perform business functions, and must be protected in accordance with the PCI DSS.
- **CVV2 storage.** The *Visa U.S.A. Inc. Operating Regulations* prohibit merchants and/or their agents from storing the Card Verification Value 2 data (security code printed within or immediately to the right of the signature panel) after transaction authorization.
- **Know your liability.** Many merchant agreements now include provisions that hold businesses liable for losses resulting from compromised card data if a business (or its service provider) lacks adequate data security.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa Rules for Returns and Exchanges

As a merchant, you are responsible for establishing the merchandise return and adjustment (credit) policies that will provide your business with maximum profitability and customer service. 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 merchant bank 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 or Returns	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 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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Disclosure for Card-Absent Merchants

Mail Order

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

Internet

Your refund and credit policies should be available to online customers through clearly visible links on your home page. You should also provide "click-through" confirmation for important elements of the policy. For example, when purchasing tickets for a sporting event, customers should be able to click on a button—(e.g., **"Accept"** or **"I Agree"**)—to acknowledge that they understand the tickets are non-returnable unless the event is postponed or cancelled.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa Rules for PIN-less Payment Brand Acceptance

Merchants need to understand and follow Visa payment acceptance rules if they elect to implement a PIN-less payment option for alternative debit cards. To this end, you are encouraged to work closely with your merchant bank to ensure that the following practices are adopted prior to system implementation.

Three Important Steps

1. Offer the Customer a Clear Payment Choice

Confusion often arises when customers believe they're paying using one payment brand, but the transaction is processed using another brand. For example, a customer who selects payment by Visa should always have that choice honored. Options such as *"Debit"* and *"Credit"* may have different meanings depending upon the customer's understanding. Selection of a payment brand provides a clear choice to the consumer. This is why it is best for merchants to provide their customers with a menu of acceptable brands.

- **For Internet merchants**, providing a menu or radio button that presents all of the payment brand options allows the customer to make an informed choice (as shown in the example to the right).
- **For telephone merchants** who instruct customers to select their preferred payment method through a Voice Response Unit (VRU) or customer service agent, identify specific payment brand options, and allow the customer to make an informed choice. Don't use generic terms, such as credit, debit and ATM.
- **For card-present merchants**, a similar payment choice option must be provided to the cardholder by the merchant.

2. Honor the Choice

If the customer indicates that he or she wants to pay with a Visa card, the merchant must make sure that choice is honored. A merchant is allowed to steer the customer to other forms of payment, but cannot confuse or mislead the customer or omit important information in the process. In other words, the choice is ultimately the customer's. A transaction can only be processed as something other than Visa if the customer has selected another form of payment. However, if a customer chooses Visa, it must be processed as a Visa transaction.

3. Confirm the Choice

To avoid any kind of misunderstanding about the customer's choice of payment, merchants should include a confirmation page or voice confirmation that specifies the payment option selected (e.g., Visa, Mastercard, Star).

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Dynamic Currency Conversion (DCC) Compliance

What is the Dynamic Currency Conversion (DCC) Service?

Dynamic Currency Conversion (DCC) is an optional service that is facilitated by a merchant at the point of sale with either a third party agent or through its merchant bank. DCC gives a Visa cardholder the choice of either paying for goods or services in their billing currency or in the merchant's pricing currency.

In a typical DCC transaction, the purchase price is converted from the merchant's pricing currency into another currency, the "transaction currency." This is the cardholder's billing currency. This conversion is performed at the point of sale, before a merchant bank presents the transaction for authorization. The transaction amount is based on a labelled price in the merchant's pricing currency and converted at a rate agreed upon by the merchant and the cardholder, plus any other charges for currency conversion.

Merchants that offer DCC generally have a high percentage of International customers, particularly those in the travel and entertainment sectors, and at tourist destinations. DCC may also be offered in card-present and card-absent transactions.

When performed correctly, DCC provides transparency for Visa cardholders. It allows a cardholder to see the transaction amount in his or her billing currency **and** the merchant's pricing currency. This way, the cardholder knows exactly how much the goods or services cost, and is able to make value judgments quickly and easily.

With DCC, there are no surprises—the amount agreed and verified by the cardholder using either a PIN or signature at point of sale is exactly the amount charged on his or her payment card statement.

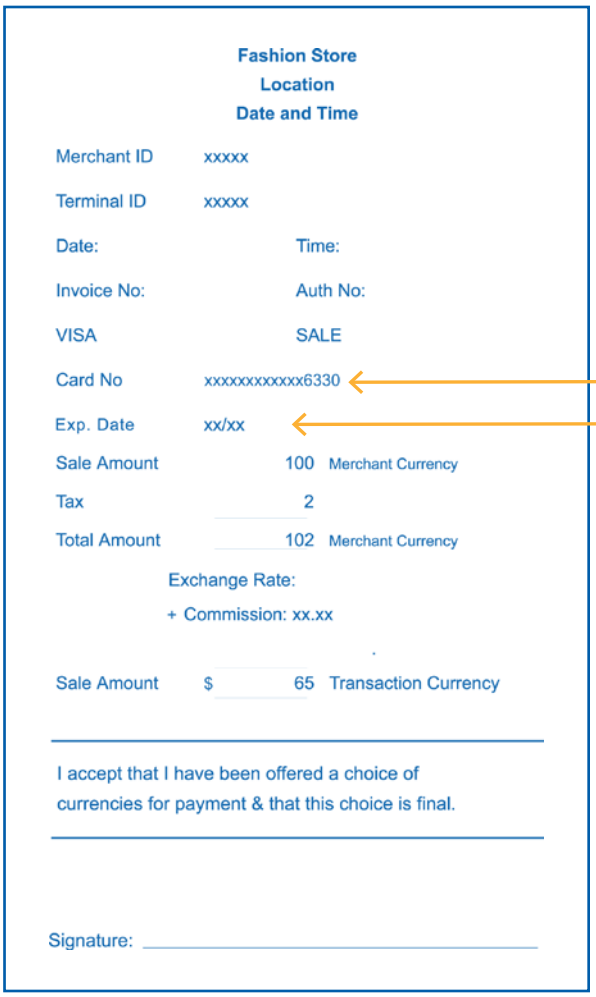
DCC is currently prohibited for ATM and cash disbursement transactions.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

DCC Transaction Receipt Requirements

For both a card-present or card-absent environment, a DCC transaction must contain all of the following:

- Transaction amount of the goods or services purchased in the merchant's local currency, including currency symbol next to the amount.
- Exchange rate, including any commission.
- Total price in the transaction currency, accompanied by the words "Transaction Currency," including currency symbol next to the amount.
- A disclaimer that:
  - is easily visible to the cardholder
  - specifies that the cardholder has been offered a choice of payment in the merchant's local currency and indicates that the cardholder understands the choice of currency is final



Truncated Account Number
Visa requires that all electronic POS terminals provide account number truncation on transaction receipts. This means that only the last four digits of an account number should be printed on the customer's copy of the receipt.

The expiration date should not appear at all. Existing POS terminals must comply with these requirements. To ensure your POS terminals are properly set up for account number and expiration date truncation, contact your merchant bank.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

DCC Transaction Receipt Best Practices

Suggested DCC best practices for merchants are as follows:

- Fully disclose to the cardholder that DCC is optional.
- A DCC transaction receipt must not contain misleading text, layout, font sizes or use of text highlighting, that may lead to cardholder confusion or disputes.
- The transaction currency and amount should be shown in a larger typeface.
- To aid confirmation of cardholder choice, a cardholder signature may be required to acknowledge cardholder agreement to participation in a DCC transaction. This is in addition to the signature or PIN verification to confirm the transaction and cardholder identity.
- Communication to the cardholder in their local language is advisable, where technically possible, or in English as the default.
- There must be a clear statement that the cardholder recognizes that he or she has been given a choice of currencies.
- There needs to be a clear statement acknowledging that the cardholder's choice of currency is final. This **does not** mean the use of the term "*No Refunds*."

DCC Restrictions

A DCC merchant:

- Must **not** use any contractual language or procedures that result in the cardholder choosing DCC transaction by default. The merchant must inform the cardholder that the service is optional.
- Must **not** convert a transaction amount in a local currency into an amount in a cardholder's billing currency **after** the transaction has been completed, but is not yet entered into the Interchange.
- Must not process a contactless "no signature required" or "small ticket" transaction.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

SECTION 2 Card-Present Transactions

What's Covered

- Doing It Right at the Point of Sale
- Visa Card Features and Security Elements
- Authorization
- Signature and Identification
- Suspicious Behavior
- Skimming
- Code 10 Calls
- Recovered Cards
- Electron Cards
- Visa Travelers Cheques

Card-present transactions are those in which both the card and cardholder are present at the point of sale. Merchants associated with this sales environment include traditional retail outlets such as department and grocery stores, electronics stores, and specialty shops and boutiques. Gas stations and other businesses where customers use unattended payment devices are also defined as card-present merchants.

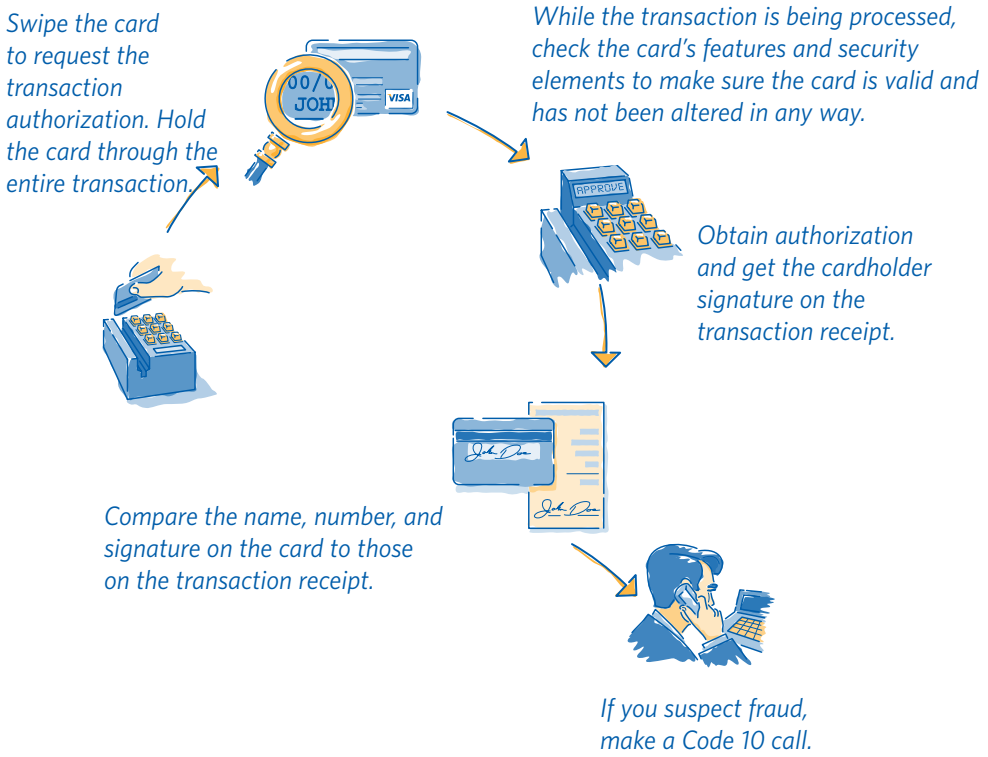
In traditional sales environments, merchants are required to take all reasonable steps to assure that the card, cardholder, and transaction are legitimate. Proper card acceptance begins and ends with sales staff and is critical to customer satisfaction and profitability.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Doing It Right at the Point of Sale

Whether sales associates are experienced or new to the job, if they follow a few basic card acceptance procedures, they will do it right the first time and every time. The illustration below provides an overview of the card acceptance steps that should be followed at the point of sale. Each step is explained in greater detail in this section.

Illustration of Card Acceptance



It Pays to Swipe the Stripe

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

Swipe the card to request the transaction authorization. Hold the card through the entire transaction.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Verifying the Account Number

Most POS terminals also allow merchants to verify that the account number embossed on the front of the card is the same as the account number encoded on the card's magnetic stripe. How you check the numbers depends on your POS terminal. In some cases, the magnetic stripe number is displayed on the terminal or the truncated account number is printed on the sales receipt. In others, the terminal may be programmed to check the numbers electronically. In such instances, you will be prompted to enter the last four digits of the embossed account number, which will then be matched against the last four digits of the account number on the magnetic stripe.

If the account number is printed on the receipt, in many cases only the last four digits will be used. If the numbers don't match, you will receive a "No Match" message. In such instances, you should make a Code 10 call.

Visa requires that all new electronic POS terminals provide account number truncation on transaction receipts. This means that only the last four digits of an account number should be printed on the customer's copy of the receipt, and the expiration date should not appear at all. Existing POS terminals must also comply with these requirements. To ensure your POS terminals are properly set up for account number truncation, contact your merchant bank. (See page 18 for a transaction receipt account number truncation example.)

If a Card Won't Read When Swiped

In some instances, when you swipe a card, the terminal will not be able to read the magnetic stripe or perform an authorization. When this occurs, it usually means one of three things:

- The terminal's magnetic-stripe reader is not working properly.
- The card is not being swiped through the reader correctly.
- The magnetic stripe on the card has been damaged or demagnetized. Damage to the card may happen accidentally, but it may also be a sign that the card is counterfeit or has been altered.

If a card won't read when swiped, you should:

- Check the terminal to make sure that it is working properly and that you are swiping the card correctly.
- If the terminal is okay, take a look at the card's security features to make sure the card is not counterfeit or has not been altered in any way (see *Visa Card Features and Security Elements* on page 25).
- If the problem appears to be with the magnetic stripe, follow store procedures. You may be allowed to use the terminal's manual override feature to key-enter transaction data for authorization, or you may need to make a call to your voice-authorization center.
- For key-entered or voice-authorized transactions, make an imprint of the front of the card. The imprint proves the card was present at the point of sale and protects your business from potential chargebacks if the transaction turns out to be fraudulent. The imprint can be made either on the sales receipt generated by the terminal or on a separate manual sales receipt form signed by the customer.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Key-entered transactions are fully acceptable, but they are associated with higher fraud and chargebacks rates. In addition, when transactions are key-entered, the benefits associated with special security features—such as the expiration date and Card Verification Value 2 (CVV2)—are not available.

How to Minimize Key-Entered Transactions

These best practices can help you keep key-entered transactions at acceptably low levels and should be incorporated into your daily operations and staff training and review sessions.

Pinpoint Areas with High Key-Entry Rates

Calculate the percentage of key-entered transactions compared to total transactions to pinpoint which stores, terminals, or sales associates have high key-entry rates. Merchants are encouraged to monitor their key-entry rates on a monthly basis.

To obtain the percentage of key-entered transactions for a particular terminal, divide the total number of key-entered transactions by the total number of sales. Exclude from both totals any mail or telephone orders that may have been made at the terminal. Perform the above calculation for each terminal and for each sales shift to determine the key-entry rate per sales associate. Repeat the process for each store, as appropriate.

Many products are available for cleaning magnetic-stripe readers. You can order Visa ReaderCleaner™ cards (VBS - MIM 01.04.03) from Visa Fulfillment at 1-800-VISA-311.

Find Causes and Look for Solutions

If your key-entry rates are greater than one percent per terminal or sales associate, you should investigate the situation and try to find out why. The following chart summarizes the most common reasons for high key-entry rates and provides possible solutions.

KEY-ENTRY CAUSE	SOLUTION
Damaged Magnetic-Stripe Readers	Check magnetic-stripe readers regularly to make sure they are working.
Dirty Magnetic-Stripe Readers	Clean magnetic-stripe reader heads several times a year to ensure continued good use.
Magnetic-Stripe Reader Obstructions	Remove obstructions near the magnetic-stripe reader. Electric cords or other equipment could prevent a card from being swiped straight through the reader in one easy movement.
Spilled Food or Drink	Remove any food or beverages near the magnetic-stripe reader. Falling crumbs or an unexpected spill could soil or damage the machine.
Anti-Theft Devices that Damage Magnetic Stripes	Keep magnetic anti-theft deactivation devices away from any counter area where customers might place their cards. These devices can erase a card's magnetic stripe.
Improper Card Swiping	• Swipe the card once in one direction, using a quick, smooth motion. • Never swipe a card back and forth. • Never swipe a card at an angle. This may cause a faulty reading.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa Card Features and Security Elements

Every Visa card contains a set of unique design features and security elements developed by Visa to help merchants verify a card's legitimacy. By knowing what to look for on a Visa card, your sales associates can avoid inadvertently accepting a counterfeit card or processing a fraudulent transaction.

Train your sales staff to take a few seconds to look at the card's basic features and security elements after they have swiped the card and are waiting for authorization. Checking card features and security elements helps to ensure that the card is valid and has not been altered in any way.

Holding Onto the Card

Sales staff should be instructed to keep payment cards in their possession during transaction processing. Holding onto the card allows time to check card features and security elements and to compare the cardholder signature on the card with the signature on the transaction receipt.

What to Look for on all Visa Cards

Cards with Visa Mini Dove Design Hologram on Back of Card

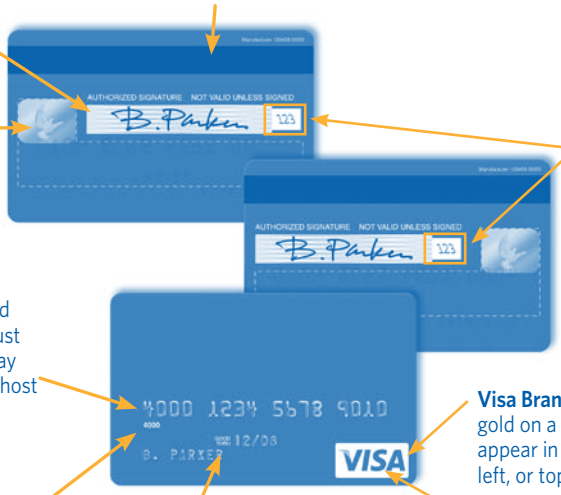
The **Signature Panel** has an updated tamper-evident design, as shown here, or has a custom design. It may vary in length depending on card type.

If someone has tried to erase the signature panel, the word "VOID" will be displayed.

The **magnetic stripe** is encoded with the card's account number, expiration date, and other identifying information.

Card Verification Value (CVV2) is a three-digit code that appears either on the signature panel or on a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-absent transactions to verify that the customer is in possession of a valid Visa card at the time of the sale.

The **Mini Dove Design Hologram** may appear on the back anywhere within the outlined areas shown in these images. A three-dimensional dove hologram should reflect light and seem to change as you tilt the card. Most counterfeit cards contain a one-dimensional printed image on a foil sticker.



Embossed or Printed Account Number on valid cards begins with "4." The account number must be even and straight. On altered cards, they may have fuzzy edges, or you may be able to see "ghost images" of the original numbers.

Visa Brand Mark appears in blue and gold on a white background. It must appear in either the bottom right, top left, or top right corner.

Ultraviolet "V" is visible over the Visa Brand Mark when placed under an ultraviolet light.

Four-Digit Number must be printed directly below the account number. This four-digit number must match exactly with the first four digits of the account number. Both must begin with a "4."

"Good Thru" (or "Valid Thru") Date is the expiration date of the card. It is located below the embossed account number. If the current transaction date is after the "Good Thru" date, the card has expired.

Always request authorization on an expired card. If the card issuer approves the transaction, proceed with the sale. Never accept a transaction that has been declined.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Cards with Visa Holographic Magnetic Stripe on Back of Card

The **Signature Panel** has an updated tamper-evident design, as shown here, or has a custom design.

The **Holographic Magnetic Stripe** should have a ring around the sun when the card is moved from side-to-side. The word "VISA" should appear in the center of the sun when the card is tilted.

If someone has tried to erase the signature panel, the word "VOID" will be displayed.

Embossed or Printed Account Number on valid cards begins with "4." The account number must be even and straight. On altered cards, they may have fuzzy edges, or you may be able to see "ghost images" of the original numbers.

Card Verification Value (CVV2) is a three-digit code that appears either on the signature panel or on a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-absent transactions to verify that the customer is in possession of a valid Visa card at the time of the sale.

Four-Digit Number must be printed directly below the account number. This four-digit number must match exactly with the first four digits of the account number. Both must begin with a "4."

Visa Brand Mark appears in blue and gold on a white background. It must appear in either the bottom right, top left, or top right corner.

"Good Thru" (or "Valid Thru") Date is the expiration date of the card. It is located below the embossed account number. If the current transaction date is after the "Good Thru" date, the card has expired.

Cards with Dove Design Hologram on Front of Card

The **magnetic stripe** is encoded with the card's account number, expiration date, and other identifying information.

If someone has tried to erase the signature panel, the word "VOID" will be displayed.

Card Verification Value (CVV2) is a three-digit code that appears either on the signature panel or on a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-absent transactions to verify that the customer is in possession of a valid Visa card at the time of the sale.

The **Signature Panel** has an updated tamper-evident design, as shown here, or has a custom design.

Embossed or Printed Account Number begins with 4. All digits must be clear, even, and the same size/shape. If a card has been re-embossed, the numbers may appear fuzzy. As a general rule of thumb, always check the hologram. It is easier to spot a re-embossed number there.

Flying Dove Hologram should appear to be three-dimensional and appear to move when the card is tilted back and forth.

Four-Digit Number must be printed directly below the account number. This four-digit number must match exactly with the first four digits of the account number. Both must begin with a "4."

Visa Brand Mark appears in blue and gold on a white background. It must appear in either the bottom right, top left, or top right corner.

"Good Thru" (or "Valid Thru") Date is the expiration date of the card. It is located below the embossed account number. If the current transaction date is after the "Good Thru" date, the card has expired.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa Flag Cards with Dove Design Hologram on Front of Card

The **Signature Panel** should be white with the word "VISA" repeated in a diagonal pattern in blue and gold print. The card account number should be printed in the panel.

The words "Authorized Signature" and "Not Valid Unless Signed" must appear above, below, or beside the signature panel.

If someone has tried to erase the signature panel, the word "VOID" will be displayed.

The **magnetic stripe** is encoded with the card's account number, expiration date, and other identifying information.

Card Verification Value (CVV2) is a three-digit code that appears on the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-absent transactions to verify that the customer is in possession of a valid Visa card at the time of the sale.

Embossed/Printed Account Number begins with 4. All digits must be clear, even, and the same size/shape. If a card has been re-embossed, the numbers may appear fuzzy. As a general rule of thumb, always check the hologram. It is easier to spot a re-embossed number there.

Flying Dove Hologram should appear to be three-dimensional and appear to move when the card is tilted back and forth.

Visa Logo should have micro-printing around the border. The fine print is barely readable without magnification.

Four-Digit Number must be printed directly below the embossed account number. This printed number must match exactly with the first four digits of the account number.

"Good Thru" (or "Valid Thru") Date is the expiration date of the card. It is located below the embossed account number. If the current transaction date is after the "Good Thru" date, the card has expired.

Ultraviolet-Sensitive Dove is visible in the face of the card when the card is placed under an ultraviolet light.

Flying "V" is an embossed security character beside the "Good Thru" date. This character is not a required security feature and may or may not appear on the card.

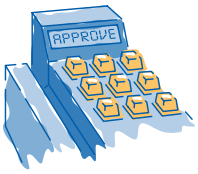
Always request authorization on an expired card. If the issuer approves the transaction, proceed with the sale. Never accept a transaction that has been declined.

When Something Doesn't Look Right

If any of the Visa card security features are missing or look altered, keep the card in your possession and make a Code 10 call to your authorization center. You may be instructed to try to recover the card or simply to return it to the cardholder and decline the transaction (see *Code 10 Calls* on page 35).

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Authorization



The authorization process allows the card issuer to approve or decline a transaction. In most cases, authorizations are processed electronically in a matter of moments. However, to protect against fraud, the card issuer may request additional information about the transaction

If properly done, authorizing a transaction is quick and easy, and protects merchants against fraud and chargebacks.

Authorization Responses

During the authorization process, your sales associates should receive one of the following responses (or one that is similarly worded).

*Authorization should be seen as an indication that account funds are available and a card has not been reported as lost or stolen. It is **not** proof that the true cardholder or a valid Visa card is involved in a transaction.*

RESPONSE	MEANING
Approved	Card issuer approves the transaction. This is the most common response, about 95% of all authorization requests are approved.
Declined or Card Not Accepted	Card issuer does not approve the transaction. The transaction should not be completed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account.
Call, Call Center, or Referrals	Card issuer needs more information before approving the sale. Most of these transactions are approved, but you should call your authorization center and follow whatever instructions you are given. In most cases, an authorization agent will ask to speak directly with the cardholder or will instruct you to check the cardholder's identification.
Pick Up	Card issuer wants to recover the card. Do not complete the transaction. Inform the customer that you have been instructed to keep the card, and ask for an alternative form of payment. If you feel uncomfortable, simply return the card to the cardholder (see *Card Recovery Procedures* on page 36).
No Match	The embossed account number on the front of the card does not match the account number encoded on the magnetic stripe. Swipe the card again and re-key the last four digits at the prompt. If a "No Match" response appears again, it means the card is counterfeit. If it can be done safely, keep the card in your possession, and make a Code 10 call.

When a transaction is approved, the POS terminal automatically prints a sales receipt. When a negative or alert message is received, the response is displayed on the POS terminal, and no sales receipt is printed. Whatever the message, you should continue to treat the customer courteously so as not to arouse alarm or suspicion.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Zero-Percent Tip Authorizations

Merchants should not estimate transaction amounts. For restaurant, taxicabs, limousine, bar, tavern, beauty/barber shop, and health/beauty spa merchants, in particular, this means debit or credit card transactions should be authorized only for the known amount of the check. **Do not add on an estimated tip.**

Cardholders today can check their account balances almost instantly via the Internet or ATMs. An authorization that includes an estimated tip can reduce their available cash or credit balance by an unrecognizable amount.

For example, a cardholder's restaurant bill is $100, but the staff adds on a 20 percent tip—that is, $20—for authorization purposes. If the cardholder only adds on a $15 tip, or leaves the tip in cash, the authorization "hold" on the larger amount may make it appear that he or she was overcharged. That, in turn, can lead to angry phone calls from an unhappy customer—and the potential for reduced business.

To ensure zero-percent tip authorization for all transactions, taxicab, limousine, bar, tavern, beauty/barber shop, health/beauty spa, and restaurant merchants should:

- **Instruct staff to authorize only for the check amount.** Your staff training and review materials should emphasize the importance of authorizing only for the known amount of the check, excluding any estimated tip.
- **Ensure your authorization system is set up for zero-percent authorization.** Check with your POS terminal provider to ensure that your terminals are programmed to authorize only for the known check amount.

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

Chargeback Protection

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 an incorrect or disputed transaction amount.

Split-Tender Transactions

A split-tender transaction occurs when a cardholder purchases goods or services with a Visa card plus some other form of payment, or tender, such as cash or check or another Visa card. Merchants set their own policies on whether or not to accept split-tender transactions. Make sure that your sales staff knows your policy.

Partial Authorizations

Partial Authorization provides an alternative to a declined transaction by permitting a prepaid card issuer to return an authorization approval for a partial amount, an amount less than the transaction amount requested by the merchant, when the available card balance is not sufficient to approve the transaction in full. The cardholder is able to use up the remaining funds on the Visa card and select another form of payment (e.g., another payment card, cash, check) for the remaining balance of the transaction. Partial Authorization benefits all stakeholders, resulting in improved cardholder satisfaction at the point of sale and increased sales.

For further information on Partial Authorizations, contact your merchant bank.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Signature and Identification

The final step in the card acceptance process is to ensure that the customer signs the sales receipt and to compare that signature with the signature on the back of the card. When signing the receipt, the customer should be within your full view, and you should check the two signatures closely for any obvious inconsistencies in spelling or handwriting.

While checking the signature, you should also compare the name, account number, and signature on the card to those on the transaction receipt.

- Match the name and last four digits of the account number on the card to those printed on the receipt.

- Match the signature on the back of the card to the signature on the receipt. The first initial and spelling of the surname must match. *Note: Embossed name and signature do not need to be the same.*

For suspicious or non-matching signatures, make a Code 10 call and ask for further instructions. *Note: If the transaction is accepted with a non-matching signature and it turns out to be fraudulent, your business may be liable, even if all other procedures were followed.*

For more information on how to make a Code 10 call, refer to page 35.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Unsigned Cards

While checking card security features, you should also make sure that the card is signed. An unsigned card is considered invalid and should not be accepted. If a customer gives you an unsigned card, the following steps must be taken:

- Check the cardholder's ID. Ask the cardholder for some form of official government identification, such as a driver's license or passport. Where permissible by law, the ID serial number and expiration date should be written on the sales receipt before you complete the transaction.
- Ask the customer to sign the card. The card should be signed within your full view, and the signature checked against the customer's signature on the ID. A refusal to sign means the card is still invalid and cannot be accepted. Ask the customer for another signed Visa card.
- Compare the signature on the card to the signature on the ID.

The words "Not Valid Without Signature" appear above, below, or beside the signature panel on all Visa cards.

If the cardholder refuses to sign the card, and you accept it, you may end up with financial liability for the transaction should the cardholder later dispute the charge.

"See ID"

Some customers write "See ID" or "Ask for ID" in the signature panel, thinking that this is a deterrent against fraud or forgery; that is, if their signature is not on the card, a fraudster will not be able to forge it. In reality, criminals don't take the time to practice signatures. They use cards as quickly as possible after a theft and prior to the accounts being blocked. They are actually counting on you not to look at the back of the card and compare signatures; they may even have access to counterfeit identification with a signature in their own handwriting.

"See ID" or "Ask for ID" is not a valid substitute for a signature. The customer must sign the card in your presence, as stated above.

Requesting Cardholder ID

When should you ask a cardholder for an official government ID? **Although Visa rules do not preclude merchants from asking for cardholder ID, merchants cannot make an ID a condition of acceptance. Therefore, merchants cannot refuse to complete a purchase transaction because a cardholder refuses to provide ID. Visa believes merchants should not ask for ID as part of their regular card acceptance procedures.** Laws in several states also make it illegal for merchants to write a cardholder's personal information, such as an address or phone number, on a sales receipt.

For more information on how to make a Code 10 call, refer to page 35.

If you are suspicious about the transaction or feel you need additional information to ensure the identity of the cardholder, make a Code 10 call.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Cash Disbursements

Generally, merchants are prohibited from making cash disbursements. Financial institutions (e.g., bank branches) may disburse cash. For these transactions, you must ask for an official government ID, and where permitted by law, you must also write the ID number and expiration date on the sales receipt. The printed four-digit number from the front of the card must also be recorded.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Suspicious Behavior

In addition to following all standard card acceptance procedures, you should be on the lookout for any customer behavior that appears suspicious or out of the ordinary.

At the Point of Sale

- Purchasing large amounts of merchandise with seemingly no concern for size, style, color, or price.
- Asking no questions or refusing free delivery on large items (e.g., heavy appliances or televisions) or high-dollar purchases.
- Trying to distract or rush sales associates during a transaction.
- Making purchases, leaving the store, and then returning to make more purchases.
- Making purchases either right when the store opens or just before it closes.

Of course, peculiar behavior should not be taken as automatic proof of criminal activity. Use common sense and appropriate caution when evaluating any customer behavior or other irregular situation that may occur during a transaction. You know what kind of behavior is normal for your particular place of business.

If you feel uncomfortable or suspicious about a cardholder or transaction, keep the card in your possession and make a Code 10 call. In any situation where making the call with the customer present feels inappropriate or unsafe, complete the transaction, return the card, and make the call immediately after the customer leaves.

At Service Stations

With their mix of attended and unattended POS devices, service stations are different from traditional retail environments. Customer behavior that signals potential fraud is also different here, both at the counter and at the pump.

AT THE COUNTER	AT THE PUMP
• Buying more than $50 worth of convenience store items • Buying large amounts of beer and cigarettes • Buying tires and not needing them mounted • Attempting to bribe a cashier • Asking for cash back with a credit card	• Activating multiple pumps • Buying gas several times a day • Filling multiple cars on the same pump • Filling large containers • Testing cards • Loitering at the pumps

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Skimming

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

Skimming often occurs in card-present environments, such as restaurants and service stations, where transaction processing may occur out of sight of the cardholder. To skim a card, fraudsters typically use a small portable device about the size of a pager. They swipe the card through the device to copy the magnetic stripe.

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

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

If you suspect skimming activity is happening at your place of business, call your merchant bank or company security **immediately**.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Code 10 Calls

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

To make a Code 10 call:

- Keep the card in your possession during the call.
- Call your voice authorization center and say, "I have a Code 10 authorization request."

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

Making Code 10 Calls After a Transaction

Sometimes a sales associate may not feel comfortable making a Code 10 call while the cardholder is at the point of sale, or the sales associate may become suspicious of a cardholder who has already left the store.

Emphasize to your sales staff that they can make Code 10 calls even after a cardholder leaves the store. A Code 10 alert at this time may help stop fraudulent card use at another location, or perhaps during a future transaction at your store.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Recovered Cards

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

- Card security features are missing or irregular, or appear to have been tampered with (see *Visa Card Features and Security Elements* on page 25).
- The account number on the magnetic stripe does not match the number embossed on the front of the card (see *Doing It Right at the Point of Sale* on page 22).
- You receive a pick-up response when a card has been swiped for electronic authorization, or you are instructed to recover the card during a Code 10 call.

Card Recovery Procedures

The following card recovery procedures apply to all Visa credit, debit, and Electron cards:

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

For cards that are inadvertently left at a merchant location and remain unclaimed, follow the procedures for contacting your merchant bank and sending in the card.

Cash Rewards

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

For Recovered Cards

- **$50 rewards:** A reward of not less than $50 will be paid for any card you recover after receiving a pick-up response to an authorization request.
- **$100 rewards:** A $100 reward is paid for cards recovered as a result of a Code 10 call, or if you determine that the first four digits of the embossed account number on a card do not match the four-digit printed number.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

For Counterfeit Information

- **$1,000 rewards:** A reward of up to $1,000 will be paid for information leading to the arrest and conviction of any person using or causing a counterfeit card to be used.

Eligibility

To be eligible for a reward, you must comply with all card-recovery procedures. If a law enforcement agency keeps the recovered card, you must provide a legible copy of the front and back of the card to your merchant bank.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Electron Cards

The Visa Electron card is a debit or prepaid card issued in countries around the world. The card is currently not issued in the United States but is accepted at many U.S. merchant locations. Like a Visa check card, the Electron card provides consumers with direct access to deposit account funds, but the card's security features and acceptance procedures are slightly different.

First, the account number on the front of an Electron card is printed, not embossed. The card also has an Electron symbol in place of the Visa dove hologram and the word "Electron," rather than "Visa," in the pattern on the signature panel. The full 16-digit account number may not be present on the front of the card. At the discretion of the card issuer, Electron cards may bear only the first and last four digits of the account number. At the discretion of the card issuer, Electron cards may be used for mail order, telephone order, or Internet purchases, or for cash advances or any other type of cash disbursement.

Electronic authorization is required for all Electron card transactions. This means you must be able to perform the authorization by swiping the card through a POS terminal. Key-entered authorizations are not allowed. If the magnetic stripe is damaged or cannot be read by the terminal, the card cannot be used.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa Travelers Cheques

Many card-present merchants also accept Visa Travelers Cheques. Visa recommends the following cheque acceptance procedures.

- Examine the cheque. Look for the key security features.
  - **Paper.** Should feel like currency. A counterfeit cheque will feel smoother or thicker.
  - **Visa Dove Watermark.** Should be visible on the front of the cheque when it is lifted to light. A counterfeit cheque will either not have a watermark, or it will be on the back rather than the front.
  - **Engraved printing.** Should have a raised texture to the touch. Engraved elements on a travelers cheque include the primary denomination indicator, the cheque border, and the cheque's portrait. A counterfeit cheque will usually have a uniformly flat surface.
  - **Silver holographic bands.** Should be to the right of Visa symbol. When the cheque is tilted, the color in the bands will appear to change; the bands also have a repeat pattern with the word "secure" in them. If the color of the bands appears black, the cheque may be counterfeit.
  - **Security inks.** Should have multicolored background pattern, with the word "Visa" and the currency and denomination included. Any attempt to alter the signature or countersignature areas will result in the smudging or disappearance of the background pattern.
- Watch the customer countersign each cheque on the lower left-hand signature line.
- Compare the countersignature with the signature on the upper right-hand signature line. In the case of dual-signature cheques, the countersignature must match one of the two original signatures in the upper right. In either case, if the signatures do not match, ask the customer to countersign the check again, on the reverse side, and ask for a photo ID.
- If you receive a cheque that is already countersigned, ask the customer to sign it on the back and request a photo ID.
- If you are suspicious about any cheque or the customer using it, call Visa's toll-free number, 1-800-227-6811, for verification and further instructions. Try to retain the cheque and customer ID, if possible, by peaceful means. If a customer becomes abusive or threatening, return the cheque and ID immediately.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

SECTION 3 Card-Absent Transactions

What's Covered

- Fraud Prevention Guidelines for Card-Absent Transactions
- Additional Fraud Prevention Tools for the Internet
- Suspicious Transactions
- Recurring Transactions

The growth of the mail order, telephone order (MO/TO), and Internet markets means increasing numbers of merchants are now processing transactions in situations where the card and cardholder are not present—and fraud may be especially difficult to detect. Of necessity, card acceptance procedures for these transactions are different from procedures for card-present transactions, but must still allow merchants to verify—to the greatest extent possible—the cardholder's identity and the validity of the purchase.

This section covers basic card acceptance procedures for both MO/TO and Internet merchants. It also includes resources and best practices that all card-absent merchants can use to prevent fraud and chargebacks.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Fraud Prevention Guidelines for Card-Absent Transactions

Visa has established a range of fraud prevention policies, guidelines, and services for card-absent merchants. Using these tools will help protect your business from fraud-related chargebacks and losses. MO/TO and Internet merchants should strongly consider developing in-house fraud control policies and providing appropriate training for their employees.

The following sections outline basic fraud prevention guidelines and best practices for card-absent merchants.

Authorize All Card-Absent Transactions

Authorization is required on **all** card-absent transactions. Card-absent transactions are considered as zero-floor-limit sales. Authorization should occur before any merchandise is shipped or service performed.

Ask for Card Expiration Date

Whenever possible, card-absent merchants should ask customers for their card expiration, or "Good Thru," date and include it in their authorization requests.

Including the date helps verify that the card and transaction are legitimate. A MO/TO or Internet order containing an invalid or missing expiration date may indicate counterfeit or other unauthorized use.

Ask for CVV2

The Card Verification Value 2 (CVV2) is a three-digit security number printed on the back of Visa cards to help validate that a customer is in possession of a legitimate card at the time of an order. (See *Visa Card Features and Security Elements* on page 25.)

Studies show that merchants who include CVV2 validation in their authorization procedures for card-absent transactions can reduce their fraud-related chargebacks, and should use CVV2 as a fraud reduction tool.

CVV2 Processing

To ensure proper CVV2 processing for card-absent transactions, merchants should:

- Ask card-absent customers for the last three numbers in or beside the signature panel on the back of their Visa cards.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

- If the customer provides a CVV2, submit this information with other transaction data (i.e., card expiration date and account number) for electronic authorization. You should also include one of the following CVV2 presence indicators, even if you are not including a CVV2 in your authorization request:

INDICATOR	WHAT IT MEANS
0	CVV2 is not included in authorization request.
1	CVV2 is included in authorization request.
2	Cardholder has stated that CVV2 is illegible.
9	Cardholder has stated that CVV2 is not on the card.

- Evaluate the CVV2 result code you receive with the transaction authorization and take appropriate action based on all transaction characteristics.

CVV2 RESULT CODE	RECOMMENDED ACTION
M – Match	Complete the transaction, taking into account all other transaction characteristics and verification data.
N – No Match	View a "No Match" response as a sign of potential fraud, which should be taken into account along with the authorization response and any other verification data. You may also want to resubmit the CVV2 to ensure a key-entry error did not occur.
P – CVV2 request not processed	Resubmit the authorization request.
S – CVV2 should be on the card, but the cardholder has reported that it isn't.	Follow up with the customer to verify that the correct card location has been checked for CVV2.
U – card issuer does not support CVV2	Evaluate all available information and decide whether to proceed with the transaction or to investigate further.

A cardholder's CVV2 may never be stored as a part of order information or customer data. The storage of CVV2 is strictly prohibited subsequent to authorization.

Verify the Billing Address with AVS

The Address Verification Service (AVS) is an automated fraud prevention tool that allows card-absent merchants to check a cardholder's billing address as part of the electronic authorization process. Studies have shown that perpetrators of fraud in card-absent transactions often do not know the correct billing address for the account they are using. Verifying the address can, therefore, provide merchants with another key indicator of whether or not a transaction is valid.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

AVS Processing

To use AVS, simply ask card-absent customers for their billing address as it appears on their monthly statement. This information is then submitted with other transaction data for electronic authorization. Address verification and authorization occur simultaneously—in a matter of seconds—and you will receive an AVS response code with the authorization.

You should evaluate the AVS response code and take appropriate action based on all transaction characteristics and any other verification information received with the authorization (i.e., expiration date, CVV2, etc.). An authorization response **always** takes precedence over AVS. Do not accept any transaction that has been declined, regardless of the AVS response.

If you a complete a transaction for which you received an authorization approval and an AVS response of "U" (unavailable), and the transaction is later charged back to you as fraudulent, your merchant bank may represent the item. U.S. issuers must support AVS or lose their right to fraud chargebacks for card-absent transactions.

Issuers also lose fraud chargeback rights for "U" responses in CVV2 request situations.

AVS RESPONSE	WHAT IT MEANS
Y – Match	Both street address and five-digit zip code match. Complete the transaction; you can be relatively confident it is legitimate.
A – Partial Match	Street address matches, but zip code doesn't. View as a sign of potential fraud. Depending on the transaction amount, you may decide to complete the transaction or investigate further to ensure it is valid.
Z – Partial Match	Zip code matches but the street address doesn't. View as a sign of potential fraud. Depending on the transaction amount, you may decide to complete the transaction or investigate further to ensure it is valid. Unless you sent only a zip code AVS request and it matched, you may want to follow up before shipping merchandise. *Note: For a zip code only request and a P.O. Box address, issuers may respond with either a "Y" (Exact Match) or a "Z" (Partial Match-Zip Code Matches).*
N – No Match	Street address and zip code don't match. View as a sign of potential fraud and take further steps to validate the transaction.
U – Unavailable	The card issuer's system is not available or the card issuer does not support AVS. The address cannot be verified at present. You must decide whether to accept or refuse the transaction, or investigate further.
R – Retry	The card issuer's system is not available; try again later. The card issuer's system may not be working. You should resubmit your AVS request later.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

International Addresses

AVS can only be used to confirm addresses in the United States, unless a card issuer supports International AVS. If you submit an address outside the U.S., you will receive the response message "G" for "Global." In such cases, you should take further steps to verify the address. You will be liable for any chargebacks if you accept the transaction, even if the card issuer approves it.

Merchant Direct Access Service (MDAS)

The Merchant Direct Access Service (MDAS) offers merchants access to AVS by dialing a toll-free number using a touch-tone phone. The service is specifically targeted to small MO/TO or Internet merchants for whom AVS may not be cost effective. Merchants using MDAS are charged on a per-transaction basis.

To use MDAS, you need a touch-tone phone with an outgoing line and a Merchant Access Code (MAC) obtained from your merchant bank. To request an address verification, call the MDAS toll-free number, **1-800-VISA-AVS (1-800-847-2287)**. An automated voice unit will guide you through the process of submitting a customer's account number and address, and give you the results of the verification.

MDAS responses are similar to AVS, but do not include a single-letter response code.

MDAS RESPONSE	WHAT IT MEANS
Exact Match	Street address and zip code match.
Partial Match	Street address matches, but not zip code.
Partial Match	Zip code matches, but not street address.
No Match	Neither street address nor zip code matches.
Retry Later	Card issuer system is not available at present.
Global	International address; cannot be verified.

Internet Transactions

Today, more and more merchants are joining the "click and mortar" market, adding online sales to their traditional card-present operations. As a result, Visa has developed guidelines and fraud prevention services especially for the web.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Merchant Website Requirements

Your merchant bank may recommend or require that you include certain content or features on your website. These elements are intended to promote ease of use for online shoppers and reduce cardholder disputes and potential chargebacks.

Merchants cannot convert transaction amounts into a different currency. Equivalent amounts in other currencies may be shown, but they must be clearly labeled as being listed for information only.

- **Complete description of goods and services.** Remember you have a global market, which increases opportunities for unintended misunderstandings or miscommunications. For example, if you sell electrical goods, be sure to state voltage requirements, which vary around the world.
- **Customer service contact information including e-mail address or phone number.** Online communication may not always be the most time-efficient or user-friendly communication method for some customers. Including a customer service telephone number as well as an e-mail address promotes customer satisfaction.
- **Return, refund, and cancellation policy.** This policy must be clearly posted. (See *Disclosure for Card-Absent Merchants* on page 15.)
- **Delivery policy.** Merchants set their own policies about delivery of goods, that is, if they have any geographic or other restrictions on where or under what circumstances they provide delivery. Any restrictions on delivery must be clearly stated on the website.
- **Country of origin.** You must disclose the permanent address of your establishment on the website. Check with your merchant bank to ensure your disclosure is made in accordance with the *Visa U.S.A. Inc. Operating Regulations* and local law.
- **Export restrictions (if known).**

Best Practices for the Web

Suggested best practices for merchant websites include:

- **Privacy statements.**
- **Information on when credit cards are charged.** You should not bill the customer until merchandise has been shipped.
- **Order fulfillment information.** State time frames for order processing and send an e-mail confirmation and order summary within one business day of the original order. Provide up-to-date stock information if an item is back-ordered.
- **Customer service time frames.** Ideally customer service e-mails or phone calls should be answered within two business days.
- **A statement on website regarding security controls used to protect customers.**
- **A statement encouraging cardholders to retain a copy of the transaction.**

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Additional Fraud Prevention Tools for the Internet

Today's e-commerce merchant has many options for combating payment card fraud. To protect your business, you need to build a reliable risk management system. Visa continues to develop online fraud-prevention tools to complement your own internal fraud avoidance efforts.

Verified by Visa

Verified by Visa is an online, real-time service that allows e-commerce merchants to validate that a cardholder is the owner of a specific account number.

The service is free to cardholders, who register their account numbers online at Visa's consumer website, *www.usa.visa.com*. Each cardholder creates a unique password at the time of registration. Then, when a cardholder makes a purchase by clicking **"Buy,"** or a similar button, on a participating merchant website, the merchant server recognizes the Visa account number and a Verified by Visa window appears. The cardholder is prompted to enter the password. The password is forwarded to the cardholder's card issuer, who confirms the cardholder's identity and the Visa account number.

Verified by Visa *participating merchants are protected by their merchant bank from receiving certain fraud-related chargebacks.*

Merchants offering Verified by Visa to their customers must incorporate a software module called a merchant plug-in (MPI) as part of their e-commerce server application. You will also need to talk with your merchant bank or gateway processor to ensure authentication-related data is included in transaction records.

Following confirmation, the Verified by Visa window disappears and the consumer is returned to the checkout screen. If the cardholder is not confirmed, an error message appears.

Fraud Screening

Today, a wide variety of fraud-screening services and practices are available to help Internet merchants assess the risk of a transaction and, in some cases, suspend processing if high-risk attributes are found. You are encouraged to develop your own internal fraud-screening programs or consider using a third party screening service, such as CyberSource Advanced Fraud Screen Enhanced by Visa.

An effective fraud-screening program will suspend processing if a transaction:

- Matches data stored in your internal negative files.
- Exceeds velocity limits and controls.
- Generates an AVS mismatch or CVV2 no match.
- Matches other high-risk attributes. For example, transactions associated with anonymous e-mail addresses, high-risk shipping addresses or cards issued outside the United States are considered high risk.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Identify low-risk transactions. *For many merchants, obtaining third party fraud scores for each and every transaction may not be cost-effective. You can minimize costs by identifying low-risk transactions—those with potential losses that are less than the cost of scoring—and eliminating them from the scoring process.*

You should also develop cost effective and timely review procedures for investigating high-risk transactions. In particular, your screening criteria should help you avoid manual review of transactions where fraud loss would be less than the cumulative costs of screening and investigation.

CyberSource Advanced Fraud Screen Enhanced by Visa

CyberSource Advanced Fraud Screen Enhanced by Visa is real-time risk management tool that evaluates the risk associated with individual transactions and provides merchants with risk scores. You use the scores as an additional means to identify potentially fraudulent orders.

Every time a cardholder clicks the **"Buy"** button on a website using CyberSource Advanced Fraud Screen, the transaction is evaluated based on over 150 data points. Running 24 hours a day, seven days a week, the service uses the world's largest database of global fraud and payment-card usage patterns, including online and offline transactions, and is updated frequently. Risk scores are calculated using a combination of neural networks, rules-based modeling, and Visa hybrid fraud technologies.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Suspicious Transactions

Card-absent merchants should develop in-house policies and procedures for handling irregular or suspicious transactions and provide appropriate training for their sales staff. Being able to recognize suspicious orders may be particularly important for merchants involved in telephone sales, and employees should be given clear instructions on the steps to take to verify these transactions.

Your sales employees should be on the lookout for any of the following signs of suspicious customer behavior:

- **Hesitation:** Beware of customers who hesitate or seem uncertain when giving you personal information such as a zip code or the spelling of a street or family name. This is often a sign that the person is using a false identity.
- **Rush orders:** Urgent requests for quick or overnight delivery—the customer who "needs it yesterday"—should be another red flag for possible fraud. While often perfectly valid, rush orders are one of the common characteristics of "hit and run" fraud schemes aimed at obtaining merchandise for quick resale.
- **Random orders:** Watch out also for customers who don't seem to care if a particular item is out of stock —"You don't have it in red? What colors do you have?"—or who order haphazardly—"I'll take one of everything!" Again, orders of this kind may be intended for resale rather than personal use.
- **Suspicious shipping address:** Scrutinize and flag any order with a ship-to address that is different from the billing address on the cardholder's account.
  - Requests to ship merchandise to post office boxes or an office address are often associated with fraud.
  - Keep lists of zip codes where high fraud rates are common and verify any order that has a ship-to address in these areas.
  - If your business does not typically service foreign customers, use caution when shipping to addresses outside the United States, particularly if you are dealing with a new customer or a very large order.

In examining what appears to be an unusual order, keep in mind that if the sale sounds too good to be true, it probably is.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Guidelines for Internet Merchants

Experience suggests that Internet orders with certain characteristics can be tip-offs to possible fraud. Suspicious online transactions are similar to suspicious sales in other card-absent environments, although the Internet offers additional opportunities for "virtual" scams. The following list of potential fraud characteristics—compiled from the advice of various experts—is offered to help you avoid being victimized by Internet fraud. An Internet transaction with any one of these characteristics by itself is seldom cause for alarm; however, a transaction with several potential risk markers may mean you are the target of a fraud scheme.

Characteristics to watch out for include:

- **First-time shopper:** Criminals are always looking for new victims. They usually hit a merchant once and don't go back a second or third time.
- **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchases. Of course, the size of "normal" orders vary from merchant to merchant.
- **Orders consisting of several of the same item:** Having multiples of the same item increases criminals' profits.
- **Orders made up of big-ticket items:** These items have maximum resale value and, therefore, maximum profit potential.
- **Orders shipped "rushed" or "overnight":** Crooks aren't concerned about extra delivery charges. They want their fraudulently obtained items as soon as possible for the quickest possible resale.
- **Orders from Internet addresses at free e-mail services:** These services have no billing relationships with their users, which in turn means no audit trail or verification that a legitimate cardholder has opened the account.
- **Orders shipped to an International address:** A significant number of fraudulent transactions are shipped to fraudulent cardholders outside of the United States. AVS can validate addresses in the United Kingdom, but other non-U.S. addresses cannot be verified.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

The next several characteristics require regular monitoring of your company's transactions. Ideally, you should have database or account history files against which to compare individual sales for possible fraud.

- **Transactions on similar account numbers:** Fraudsters often use account numbers that have been generated with software available on the Internet, such as CreditMaster.
- **Orders made on multiple cards but shipped to a single address:** These orders can also be characteristic of a software-generated account number or may have been made using a batch of stolen cards.
- **Multiple transactions on one card over a very short period of time:** Criminals often attempt to run up purchases on a single card until the account is closed.
- **Multiple shipping addresses:** In a similar fraud scenario, multiple transactions are charged to one card or similar cards that have a single billing address but multiple shipping addresses. This situation could be a sign of some organized activity, rather than one individual at work.
- **Multiple cards from a single IP address:** The Internet Protocol (IP) address identifies the computer in a network from which an order has been made. In this instance, fraud indicators may include multiple orders using different names, addresses, and card numbers, but coming from one IP address.

What To Do If You're Suspicious

Card-absent merchants should establish procedures for responding to suspicious transactions. Your sales staff should be familiar with these procedures and receive regular training on them.

Mail Order/Telephone Order Merchants

For suspicious MO/TO transactions, you should:

- **Ask for a Code 10 Authorization:** A separate phone call to your authorization center asking for a Code 10 authorization lets the center know you have concerns about a transaction. (For more information, see *Code 10 Calls* on page 35.)
- **Ask the customer for additional information:** For example, ask for day and evening phone numbers and call the customer back later. Some merchants ask for the bank name on the front of the card.
- **Separately confirm the order with the customer:** Send a note to the customer's billing address, rather than the shipping address.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

When requesting additional information to verify orders, telephone order employees should use a conversational tone so as not to arouse customers' suspicions. If a customer balks or asks why the information is needed, employees should say they are trying to protect cardholders from the high cost of fraud.

Internet Merchants

For suspicious transactions, Internet merchants should establish effective procedures for cardholder verification calls. Contacting customers directly not only reduces fraud risk, but also builds customer confidence and loyalty. Your verification procedures should address the need both to identify fraud and leave legitimate customers with a positive impression of your company.

- Use directory assistance or Internet search tools—not the telephone number given for a suspect transaction—to find a cardholder's telephone number.
- Confirm the transaction, resolve any discrepancies, and let the cardholder know that you are performing this confirmation as a protection against fraud.

The Best Advice of All

Trust your instincts! If a sale seems too good to be true, it probably is. We hear all too often that what a merchant thought was a great sale turned out to be fraud. So take the time to check out that huge order that is being shipped halfway around the world to a customer with whom you've never done business. A little bit of extra work may protect you from being the victim of a fraud scheme.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Recurring Transactions

A recurring transaction is one in which a cardholder authorizes a merchant to automatically charge his or her account number for the recurring or periodic delivery of goods or services. A typical recurring transaction might be an automatic bill pay for Internet or cable television services, a monthly newspaper subscription, or a health club membership.

Because these transactions are processed automatically, without direct participation of the cardholder, they are particularly liable to potential disputes and copy requests. The following sections provide recommendations for merchant policies and procedures to minimize such problems.

For First Recurring Transactions

An initial, or set-up, recurring transaction should be processed the same as any MO/TO or Internet transaction. If set up by mail or telephone, you should submit AVS and CVV2 queries with the authorization. For online transactions, cardholder identity should be authenticated with Verified by Visa.

The sales receipt for an initial recurring transaction must include the following information:

- The phrase "recurring transaction."
- The frequency of the debits.
- The period of time the cardholder has agreed to for the debits.

Setting Up Recurring Transactions by E-Mail

Visa allows Internet merchants to accept an electronic record, such as an e-mail message, as cardholder permission to set up a recurring transaction. This record should be kept on file for the duration of the arrangement and provided to the card issuer upon request.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

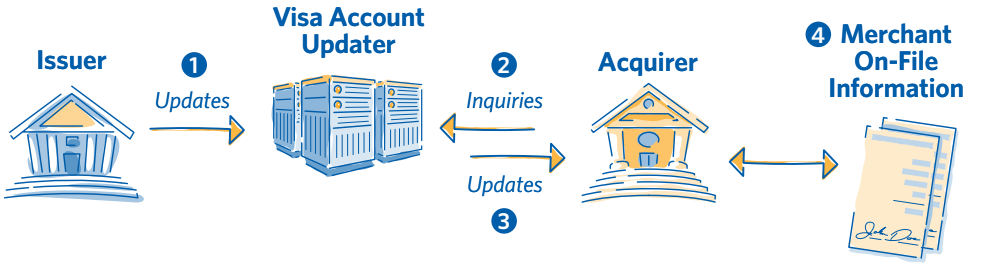
For All Recurring Transactions

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, merchant banks, and issuers to exchange electronic updates of cardholder account information.
- Keep the cardholder's expiration date on file and include it in all authorization requests.
- Use AVS.
- Ensure that all recurring transactions are clearly identified as such. For example, where a recurring transaction is set up by mail or telephone, it should have a MO/TO E-Commerce Indicator of 2. This identification is usually handled automatically by a merchant's transaction-processing system; however, you should check with your merchant bank to confirm that your system is properly set up.
- Notify the customer before billing. Cardholders should be routinely notified of regular recurring payments charged to their Visa account at least 10 days in advance. The advance notification should include the amount to be charged to the account and where necessary, alert the cardholder if the transaction amount exceeds a pre-authorized range.

VAU service ensures that merchant on-file information (cardholder account number, expiration date, status, etc.) is current. VAU allows Visa merchants, merchant banks, 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 merchant bank *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 merchant bank for each inquiry, including updated information.*

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

- Put proper controls in place to protect any stored cardholder information related to the transaction.
- Do **not** store CVV2 data. This is strictly prohibited.
- Request the cardholder's Visa account number only as payment for goods or services. The merchant must not use the account number for age verification or any purpose other than payment.
- Check customer logs daily for complaints, especially those relating to transaction amounts or failure to notify customers in advance of a recurring transaction that exceeds the pre-authorized amount range. Follow up with the customer.

Cancelling Recurring Transactions

To cancel a recurring transaction, merchants should:

- Check customer logs daily for cancellation or non-renewal of services paid for with a recurring transaction. Comply with all cancellation and non-renewal requests in a timely manner and notify the cardholder that the recurring payment account has been closed.
- Process all credits promptly. If a cancellation request is received too late to prevent the most recent recurring charge from being posted to the cardholder's account, submit the credit and notify the cardholder.
- Provide the customer with a cancellation number.

For more information on recurring transactions, see *Appendix 1: Training Your Troops*, pg. 131 to order *Merchant Best Practices for Recurring Transactions* (VRM 03.03.06).

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

SECTION 4 Payment Card Industry Data Security Standard and PIN Security and Key Management

What's Covered

- PCI DSS Requirements
- Visa PIN Security and Key Management Compliance Program
- Merchant PIN Security and Key Management—Essential Best Practices and Requirements
- Additional Security Requirements
- Steps and Requirements for Compromised Entities

With recent media reports of hacker incidents, stolen credit card and PIN numbers, and identity theft, consumers are increasingly concerned about information security. Today, consumers want absolute assurance from the merchants with whom they do business that their bankcard account number and other personal information are securely protected.

To address these concerns, Visa established the *Visa Cardholder Information Security Program (CISP)* and the *Visa Personal Identification Number (PIN) Security and Key Management Compliance Program*.

CISP is based upon the *Payment Card Industry (PCI) 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. These 12 requirements are the foundation of Visa's CISP.

Separate from the mandate to comply with PCI DSS, is the validation of compliance. Validation identifies vulnerabilities and ensures that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined merchant and service provider compliance validation levels based on the volume of transactions, the potential risk, and exposure introduced into the Visa system.

PIN Security and Key Management Compliance Program is based on the *PCI PIN Security Requirements* and is a global program designed to support all members, merchants, and service providers in the PIN acceptance transaction processing chain to maintain the highest level of PIN security.

More information about the PCI DSS, including Visa's validation requirements and a suite of security tools and resources to support compliance, are available at *www.visa.com/cisp*. For information on the *PCI PIN Security and Key Management Requirements*, go to *www.visa.com/pinsecurity.*

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

PCI DSS Requirements

The PCI DSS reflects a "walls of security" philosophy in which no single security measure should ever be relied on to provide complete protection from trespassers. Rather, risk of intrusion is minimized by erecting multiple layers of security measures that work together.

The PCI Data Security Standard consists of 12 basic requirements supported by more detailed sub-requirements:

PCI DATA SECURITY STANDARD	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect shared data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Who Must Comply

Compliance with PCI DSS applies to any entity—meaning any merchant or service provider including Third Party Agents (TPA)—that stores, processes, or transmits Visa cardholder information. All eligible merchants and service providers, regardless of size (or in the case of service providers, whether they support issuing or merchant activity) **must** comply with the Payment Card Industry Data Security Standard (PCI DSS).

Beyond basic data security, full implementation of the PCI DSS benefits merchants in several ways.

- **Customer service.** Customers seek out merchants they feel are "safe." Confident consumers are loyal customers. They come back again and again, and share their experiences with others.
- **Cost containment.** By protecting your customers, you also minimize your own exposure to risk and reduce the direct and operational costs associated with compromised cardholder information.
- **Public image.** Information security is a frequent topic of media attention. An incident of data loss or compromise not only hurts your customers, it can seriously damage your public image.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa PIN Security and Key Management Compliance Program

Visa has worked with many member financial institutions, and industry standards organizations to create security standards for the protection of PINs accepted at Automated Teller Machines (ATMs) and Point-of-Sale (POS) PIN-Entry Devices (PEDs). The Visa PIN Security and Key Management Compliance program is based on the Payment Card Industry (PCI) PIN Security Requirements, a set of mandatory requirements for the secure management, processing and transmission of cardholder PINs during transaction processing at ATMs and Point-of-Sale (POS) PIN-Entry Devices (PEDs).

The program is designed to protect members, merchants, and service providers. It is designed to ensure the safe management, processing and transmission of cardholder PINs at ATM and POS PEDs. As a result, members, merchants, and service providers avoid potential liability and losses related to a PIN compromise. The program objectives are to:

- Build a culture of security to protect cardholder PINs by requiring compliance PIN Security requirements for all participants.
- Protect payment system participant's reputation by reducing vulnerability to threats.
- Maintain cardholder confidence in the payment system.

For more information and to further assist members, merchants, and service providers in understanding and complying with these requirements, Visa offers a series of one-day key management workshops as well as a three-day PIN Security Compliance Validation Training that provide up-to-date information on the secure management and use of cryptographic keys used in ATMs, POS PIN pads, cash dispensers and hardware security modules. Workshops are available throughout the year, for workshop schedules or to enroll, visit *www.visa.com/cisp* or e-mail *pinusa@visa.com*.

For more information regarding the PCI PIN Security Requirements, visit *www.visa.com/pinsecurity.*

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Merchant PIN Security and Key Management—Essential Best Practices and Requirements

All members, merchants, and service providers in the transaction processing chain that manage cardholder PINs and encryption keys must be in full compliance with the PCI PIN Security Requirements. Of the 32 requirements detailed on *www.visa.com/pinsecurity*, there are six critical areas where merchant non-compliance could potentially subject the Visa/Interlink payment system to an extremely high level of risk.

Merchants should review the requirements below to validate their level of compliance and refer to the PCI PIN Security Requirements Manual located on *www.visa.com/pinsecurity*, as needed.

- **Use Compliant Equipment.** Purchase only terminals that have been PCI approved. Work with your merchant bank or Encryption and Support Organization (ESO) to create a plan that ensures all deployed attended POS PEDs are Visa-approved and are using Triple Data Encryption Standards (TDES) by July 2010. For more information on Visa's PED testing and TDES usage requirements, visit *www.visa.com/pin*. Visa/Interlink-accepting merchants must only deploy PEDs listed on the PCI PIN-Entry Device Approval List at *www.pcisecuritystandards.org/pin*.
- **Do Not Log PIN Blocks.** Although PINs are protected in an encrypted or enciphered form within a transaction message, they must not be retained in transaction journals or logs subsequent to PIN transaction processing. Many processing environments have programs that actively overwrite or mask PIN blocks; however, any processor of PIN-based transactions must evaluate all inbound and outbound PIN-based messages to ensure that there is no systematic logging of PIN blocks within any system. In addition, any temporary logging function for transaction research or troubleshooting must include the active removal of PIN blocks. This requirement helps prevent harvesting and subsequent attacking of any large repository of logged encrypted PINs. For further information, refer to (1) PCI PIN Security Requirements, (2) and the PCI Payment Application Data Security Standards.
- **Always Maintain Secure Key Loading Procedures.** When POS PEDs and host security modules are first initialized, they must be securely loaded with encryption keys. Regardless of the type of tamper-resistant security modules being initialized, the principles of split knowledge and dual control must be in place at all times to maintain the secrecy of the key being entered. In addition, merchants must establish procedures that prohibit any one person from having access to all components of a single encryption key. If a merchant uses an ESO for key injection into PEDs, the merchant bank must register the ESO with Visa. For more information, refer to the *Visa Cryptographic Key Injection Facility Requirements Manual* at *www.visa.com/pinsecurity*.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

- **Only Use Keys for a Single Purpose.** To limit the magnitude of exposure should any key be compromised, encryption keys must be used only for their sole intended purpose. This applies to all keys used in POS PED and network processor links. Production keys must never be shared or substituted within an entity's test system. All master keys or hierarchy keys used in any production or test environment must be unique and separate for each environment. Use of any production key in a test system is a high-risk violation. Any production key exposed in the test system or any key that has been encrypted using such exposed keys should be considered compromised and should be immediately replaced.
- **Ensure All Devices Have Unique Keys.** Cryptographic keys residing within a PED must be unique to that device. This includes initialization keys, key-exchange keys, and PIN-encryption keys. By ensuring that these keys are unique to each device, a merchant can make sure their PEDs are unattractive targets for an attack. This is because a unique key that has been "cracked" exposes only those PINs that were actually entered at the attacked device. Conversely, compromise of a key used for a large number of devices could expose all PINs entered at all of those devices. When validating compliance with this requirement, technical staff should also look for weak keys (known as default, predictable, or simple keys).
- **Visa/Interlink TDES mandate.** Merchants should establish detailed plans to ensure Visa's PED-testing and TDES usage dates are met by July 2010. Failure to comply could result in a high degree of risk exposure. For more information, visit *www.visa.com/pin.*

For more information or questions contact your merchant bank or send an e-mail to *pinusa@visa.com.*

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Additional Security Requirements

Merchants should also be aware of the following data security requirements and best practices:

- **Minimize Cardholder Data Retention and Eliminate Magnetic Stripe Data Storage**. The *Visa U.S.A. Inc. Operating Regulations* prohibit merchants and/or their agents from storing the full contents of the magnetic stripe after transaction authorization. Storage of some data elements from the magnetic stripe is permitted, including the cardholder's name, primary account number, expiration data and service code.However, these values should only be stored if needed to perform business functions, and must be protected in accordance with the PCI DSS.
- **CVV2 storage.** The *Visa U.S.A. Inc. Operating Regulations* prohibit merchants and/or their agents from storing the Card Verification Value 2 data (security code printed within or immediately to the right of the signature panel) after transaction authorization.
- **Know your liability.** Many merchant agreements now include provisions that hold businesses liable for losses resulting from compromised card data if a business (or its service provider) lacks adequate data security.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Steps and Requirements for Compromised Entities

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry (PCI) Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS), and PCI PIN Security Requirements.

Key Point to Remember

To minimize the impact of a cardholder information security breach, Visa has put together an Incident Response Team to assist in forensic investigations. In the event of a compromise, Visa will coordinate a team of forensic specialists to go onsite immediately to help identify security deficiencies and control exposure. The forensic information collected by the team is often used as evidence to prosecute criminals.

1. **Immediately contain and limit the exposure to minimize data loss.** Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation:
   - Do not access or alter compromised system(s) (i.e., don't log on at all to the compromised system(s) and change passwords, do not log in as ROOT).
   - Do not turn the compromised system(s) off.Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
   - Preserve logs (i.e., security events, web, database, firewall, etc.)
   - Log all actions taken.
   - If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection with the exception of any systems believed to be compromised.
   - Be on "high" alert and monitor traffic on all systems with cardholder data.
2. **Alert all necessary parties immediately.** Be sure to contact:
   - Your internal incident response team and information security group.
   - If you are a merchant, contact your merchant bank.
   - If you do not know the name and/or contact information for your merchant bank, notify Visa Cyber Security and Investigations at (650) 432-2978, or *usfraudcontrol@visa.com.*
   - Your local office of the Secret Service.
3. **Provide all compromised Visa, Interlink, and Plus accounts to your merchant bank or Visa within 10 business days.** All potentially compromised accounts must be provided and transmitted as instructed by your merchant bank and Visa. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

4. **Within 3 business days of the reported compromise, provide an Incident Report document to your merchant bank.**

Note: If Visa deems necessary, an independent forensic investigation by a Visa-approved Qualified Incident Response Assessor (QIRA) will be initiated on the compromised entity.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

SECTION 5 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 merchant bank associated with the transaction.

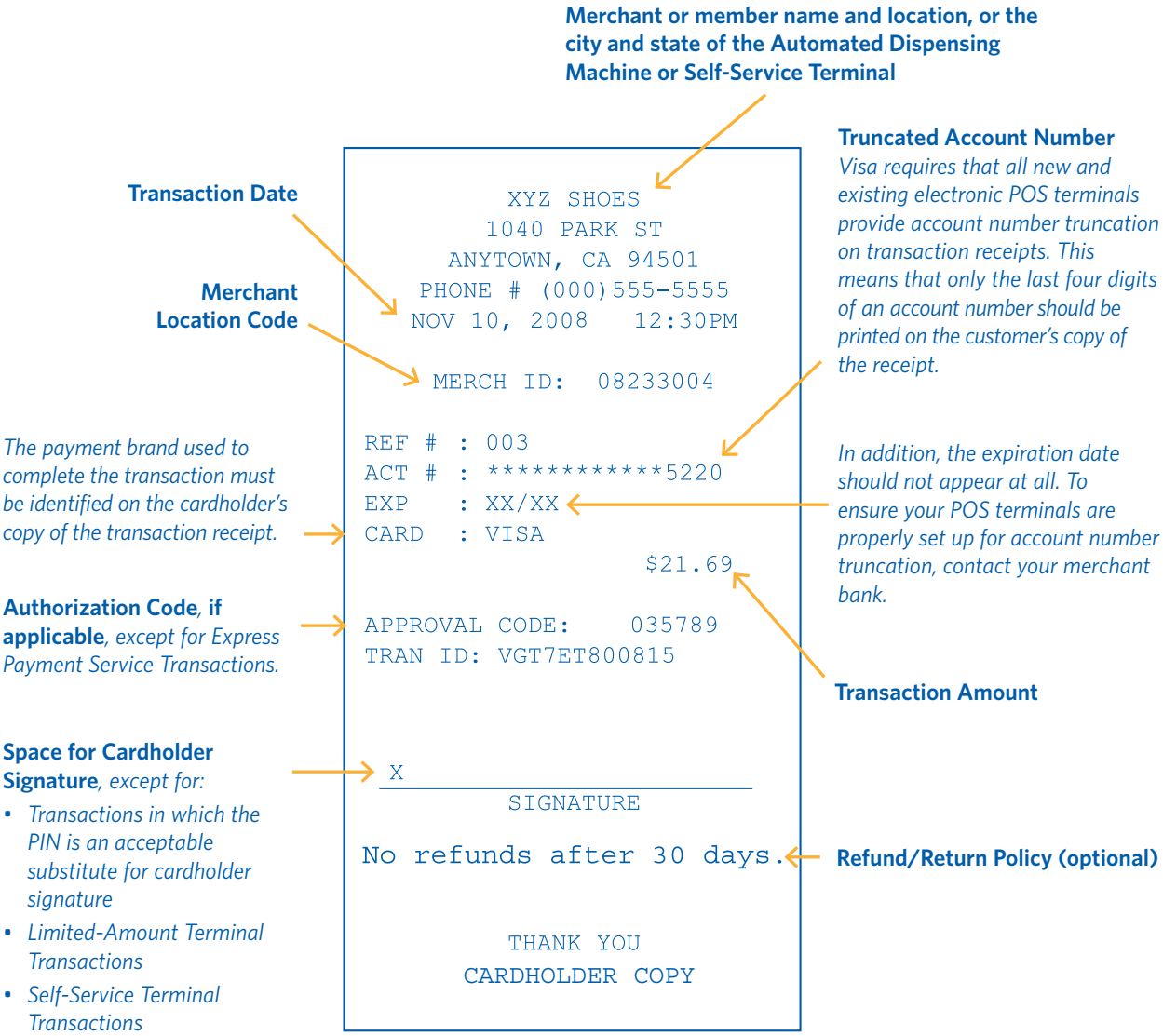
If your transaction receipts are stored at your merchant bank, the bank fulfills the copy request. However, if you store your own transaction receipts, the merchant bank forwards the request to you. You must then send a legible copy of the transaction receipt to the merchant bank, which sends it on to the card issuer.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Transaction Receipt Requirements—Card-Present Merchants

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

Electronic Point-of-sale Terminal Receipts

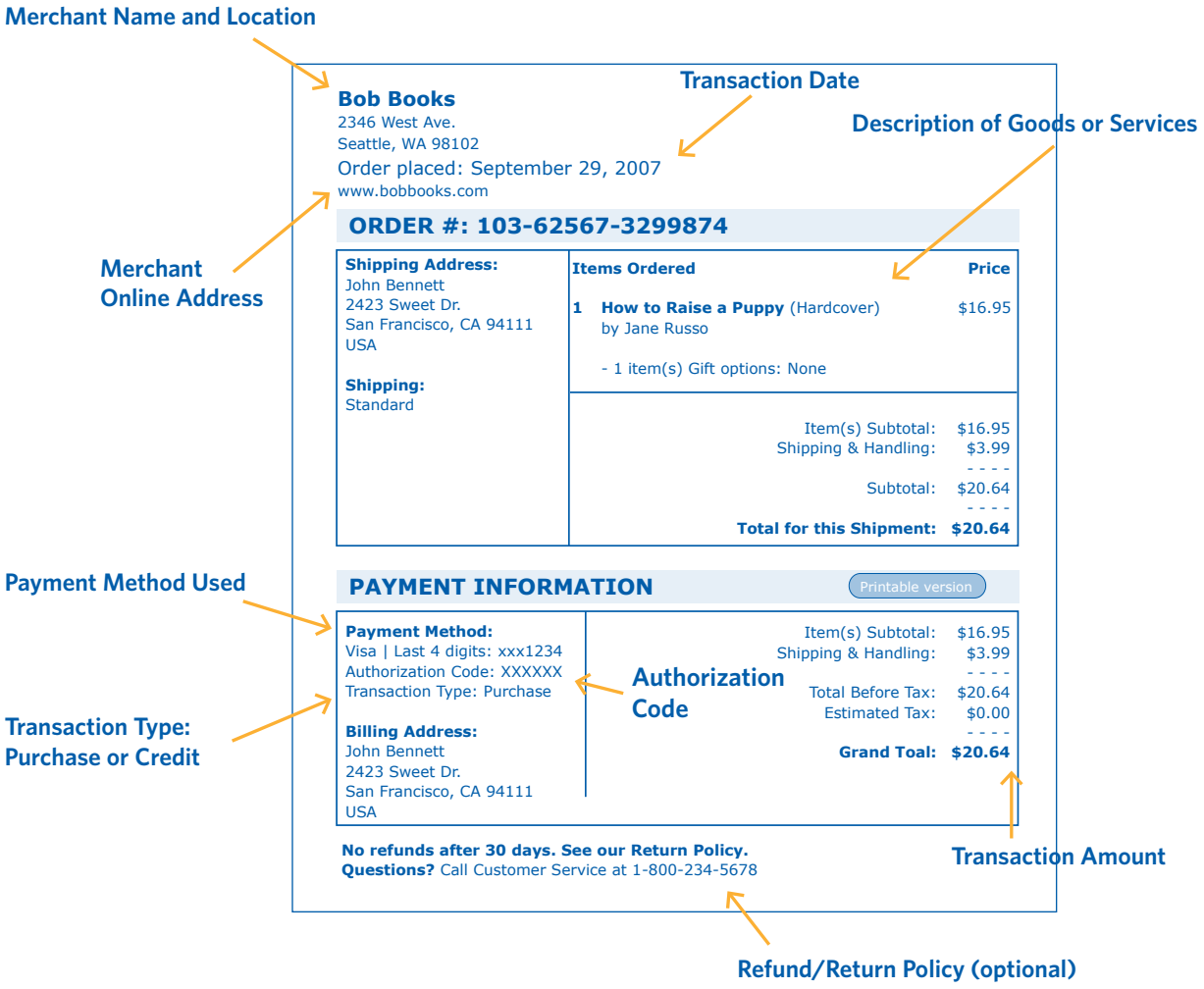


©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Transaction Receipt Requirements—Card-Absent Merchants

The following are Visa requirements for all manually printed transaction receipts.

Manual Transaction Receipts



©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Responding to Copy Requests

The illustration on the next page shows the copy request process. When a card issuer sends a copy request to a merchant bank, 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 merchant bank sends the request to you, it will tell you the number of days you have to respond. You must follow the merchant bank'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 merchant bank within the specified time frame. Your merchant bank 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 merchant bank, 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 12 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

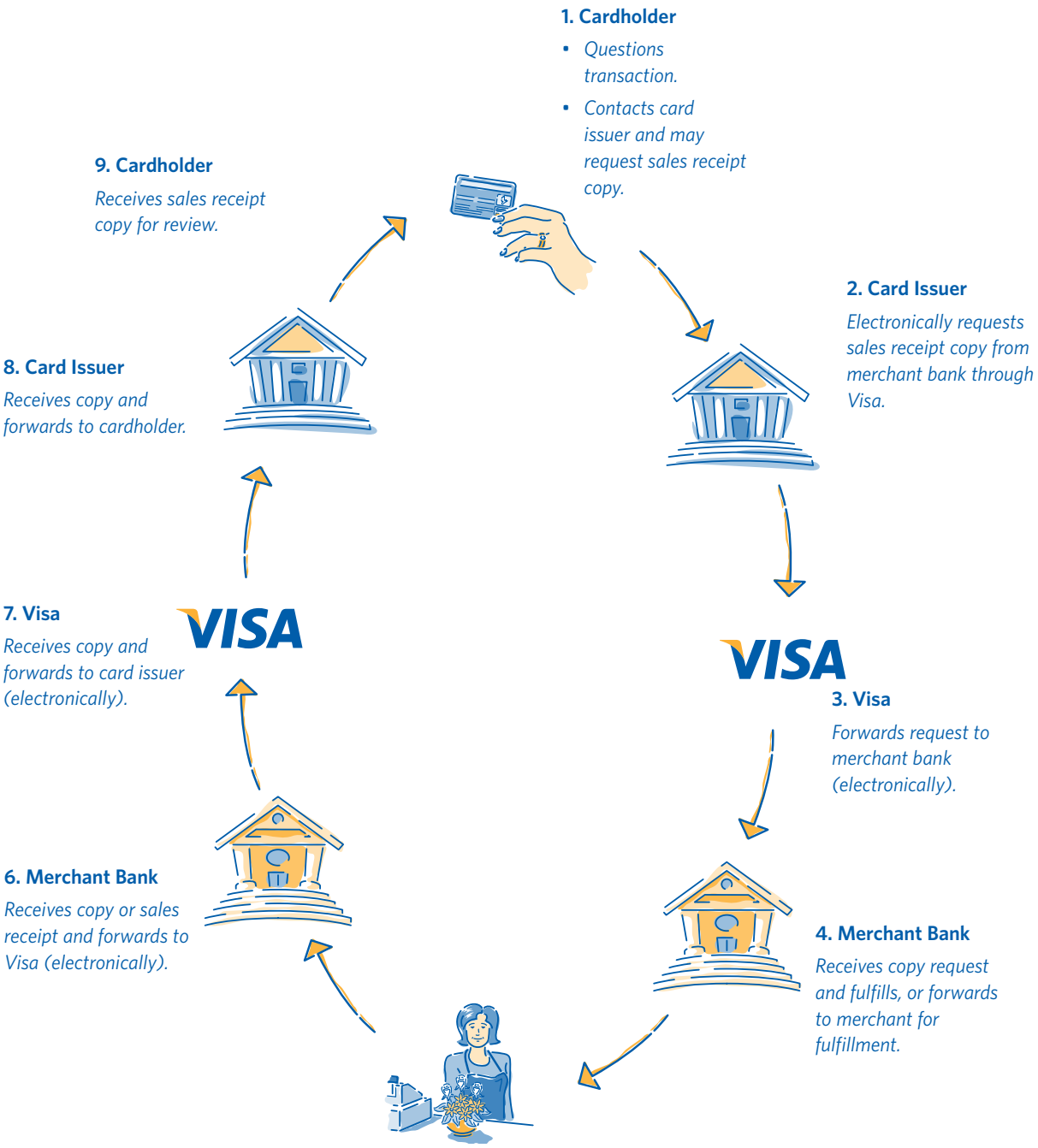
Responding to copy requests saves you time and money. As a merchant, you should always:

- Fulfill any copy requests you receive.
- Fulfill requests in a timely manner.
- Ensure that the receipt copy you send is legible.

A copy request that is unfulfilled or late can only be charged back if the retrieval request was for Reason Code 33 "Fraud" or the "true dispute reason" must be presented. Avoiding chargebacks can help you improve your customer service and profitability.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

The Copy Request Process



©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

How to Minimize Copy Requests

Merchants who keep copy requests to a minimum are more likely to have lower chargeback rates and higher profitability. 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 merchant bank to be sure it has the correct information on your "Doing Business As" (DBA) name, city, and state. 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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 best practices in the next section.)
- 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 merchant bank. If the receipt is not legible to begin with, the copy that the bank 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, silver-backed, or carbonless paper carefully.**

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

SECTION 6 Chargebacks

What's Covered

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

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

- 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 debits the merchant bank for the dollar amount of the transaction.
- The merchant bank will, most often, deduct the transaction dollar amount from the merchant's account. The merchant loses the dollar amount of the transaction.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Why Chargebacks Occur

The most common reasons for chargebacks include:

- Customer disputes
- Fraud
- Processing errors
- Authorization issues
- Nonfulfillment of copy requests (only if fraud or illegible)

Although you probably cannot avoid chargebacks completely, you can take steps to reduce or prevent them. Many chargebacks result from easily avoidable mistakes, so the more you know about proper transaction-processing procedures, the less likely you will be to inadvertently do, or fail to do, something that might result in a chargeback (see *Avoiding Chargebacks* on page 82).

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

Your Responsibility

From the administrative point of view, the main interaction in a chargeback is between a card issuer and a merchant bank. The card issuer sends the chargeback to the merchant bank, 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 7, Chargeback Reason Codes*.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

The Chargeback Life Cycle

The following illustration shows the chargeback life cycle.

1. Cardholder

- *Disputes transaction.*
- *Contacts card issuer with disputed information.*

2. Card Issuer

Reviews eligibility of transaction for chargeback. If appropriate, returns transactions (charges it back) to merchant bank through Visa (electronically).

3. Visa

- *Electronically screens chargeback for technical criteria compliance.*
- *If appropriate, forwards chargeback to merchant bank (electronically).*

4. Merchant Bank

Receives chargeback and resolves issue, or forwards to merchant.

5. Merchant

- *Receives chargeback.*
- *If appropriate, and under certain conditions, can re-present chargeback to its merchant bank.*
- *If conditions aren't met, merchant may have to accept chargeback.*

6. Merchant Bank

Forwards re-presented item to Visa.

7. Visa

- *Electronically screens re-presentment for technical criteria compliance.*
- *If appropriate, forwards re-presentment to card Issuer (electronically).*

8. Card Issuer

Receives re-presented item and, if appropriate, re-posts to cardholder's account. If chargeback issue is not appropriately addressed, card issuer may submit dispute to Visa.

9. Cardholder

Receives information resolving initial dispute and may be re-billed for item or receives credit.

Arbitration

If the card issuer disputes a representment from the merchant bank, 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 merchant bank. During arbitration, the Visa Arbitration Committee 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 committee review if members incur a loss and a valid chargeback or representment is unavailable.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Invalid Chargebacks

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.

Responding to the needs of card issuers, merchant banks, 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 merchant bank never see it. Many merchant banks 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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Chargeback Remedies

Even when you do receive a chargeback, you may be able to resolve it without losing the sale. Simply provide your merchant bank 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 merchant bank in a timely manner.

The key in this and similar situations is always to send your merchant bank as much information as possible to help it remedy the chargeback. With appropriate information, your merchant bank 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 merchant bank do not respond during the time specified on the request—which may vary depending on your merchant bank—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.

Represent-ment Rights for Card-Absent Merchants

Card-absent merchants should be familiar with the chargeback representment rights associated with the use of Address Verification Service (AVS), Card Verification Value 2 (CVV2), and the option to provide compelling information. Specifically, your merchant bank 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 U.S. 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 from a U.S. card issuer. This response means the card issuer does not support CVV2.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Verified by Visa *participating merchants are protected by their merchant bank from receiving certain fraud-related chargebacks, provided the transaction is processed correctly. If you are not participating in Verified by Visa at this time, see pg. 47 for more information.*

- 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 merchant bank to ensure that all supporting evidence for the representment is submitted.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Avoiding Chargebacks

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.

Point of Sale

- **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.
- **Expired Card.** Do not accept a card after its "Good Thru" or "Valid Thru" date.
- **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. Avoid capturing 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 cardholder signs the receipt, the transaction may be charged back to you if the receipt does not have an imprint of the embossed account number and expiration date.
- **Cardholder Signature.** The cardholder's signature is required for all card-present transactions, except for qualified small-ticket transactions. Failure to obtain the cardholder's signature could result in a chargeback if the cardholder later 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.
- **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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

- **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.
- **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.

"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.

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 merchant bank.
  - Deposit the same transaction with more than one merchant bank.
- **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 merchant bank 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 merchant bank as quickly as possible, preferably the same day the credit transaction is generated.
- **Ship Merchandise Before Depositing Transaction.** For card-absent transactions, do not deposit sales receipts with your merchant bank 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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

- **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 customer service, advise the customer in writing that the service, subscription, or membership has been cancelled and state the effective date of the cancellation.

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 limited or no refund policy must be displayed on a screen that requires the cardholder to "click and accept" the terms of your policy. This policy page cannot be bypassed.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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 retail merchants as the card is not swiped, which increases liability for chargebacks.

General recommendations for chargeback monitoring include:

- **Track chargebacks and representments 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 representment.**
- **Track card-present and card-absent chargebacks separately.** If your business combines traditional retail with card-absent transactions (MO/TO or Internet), 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 merchant banks when any one of their merchants has excessive chargebacks.

Once notified of a merchant with excessive chargebacks, merchant banks 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 merchant bank to develop a detailed chargeback-reduction plan.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Visa has three chargeback monitoring programs:

1. Merchant Chargeback Monitoring Program (MCMP)

The Merchant Chargeback Monitoring Program (MCMP) monitors chargeback rates for all merchant banks and merchants on a monthly basis. If a merchant meets or exceeds specified chargeback thresholds, its merchant bank 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 merchant banks that fail to reduce excessive merchant-chargeback rates.

2. 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 merchant bank immediately if a merchant has an excessive chargeback rate.

3. 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 merchant bank immediately if a merchant has an excessive chargeback rate.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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 U.S.A. Inc. 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 cardholder stays at a lodging merchant and is later billed as a no-show from the same location, for the same date.
- 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 issuer initiated a chargeback.
- The merchant insists that the cardholder sign a blank sales draft before the final dollar amount is known.
- The cardholder is billed for an advance deposit and the deposit amount is **not** applied toward the balance of the stay.
- A merchant that does not hold a Visa account through a merchant bank processes a transaction through another Visa merchant.
- The merchant fails to compare the signature on the card to the signature on the transaction receipt.
- The cardholder was credited more than once for the same transaction.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Compliance Resolution

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

SECTION 7 Chargeback Reason Codes

The chargebacks discussed in this section are grouped into six classifications:

- Non-Receipt of Information
- Fraud Codes
- Authorization Errors
- Processing Errors
- Cancelled or Returned
- Non-Receipt of Goods or Services

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

These classifications are designed to help you understand the underlying business reason for a chargeback. In addition, the following information is included for each type of chargeback.

- **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 merchant banks 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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Within each of these categories, the suggestions and recommendations for merchant action are further classified by action type.

- **(PR) Possible Remedy.** Steps you could take to help your merchant bank 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 appendix is current as of the date of printing. However, chargeback procedures are frequently updated and changed. Your merchant agreement and *Visa U.S.A. Inc. Operating Regulations* take precedence over this guide or any updates to its information. For a copy of the *Visa U.S.A. Inc. 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 6: Chargebacks*.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Non-Receipt of Information

Reason Code 60: Request Copy Illegible or Invalid

Definition

The card issuer requested a copy of the sales receipt and received an illegible copy, or an incomplete substitute receipt, or something other than the requested item.

Most Common Causes

The merchant submitted a substitute sales receipt that did not contain all of the required information, or the transaction receipt was not legible or was other than the requested item 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.
- The document submitted was not the requested copy of the sales receipt.

Merchant Actions

Back-Office Staff

Legible or Complete Copy

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

Incomplete Sales Receipt

(NR) If information is missing or a legible copy of the sales receipt cannot be provided, accept the chargeback. (See page 72 of this guide for further details regarding legible receipts.)

Incomplete Sales Receipt—Fraud

If a retrieval request is fraud-related and the merchant provides an incomplete or invalid substitute sales receipt, accept the chargeback. The merchant has no representment rights unless the card issuer's chargeback is for "illegible item received."

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 60: Request Copy Illegible or Invalid (continued)

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.

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- or silver-back paper carefully. Silver-back paper appears black when copied. 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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 75: Cardholder Does Not Recognize Transaction

Definition	The card issuer received a complaint from a cardholder stating that the transaction appearing on the billing statement is not recognized. This 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 merchant bank to ensure your merchant name, city, and state are properly identified in the clearing record.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Fraud Codes

Reason Code 57: Fraudulent Multiple Transactions

Definition

The card issuer received a written 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 recurring payments or 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 merchant bank evidence of the credits.

Cardholder Participated in Multiple Transactions

(PR) If the cardholder did participate in more than one valid transaction, provide your merchant bank 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 62: Counterfeit Transaction

Definition

The card issuer received a written complaint from the cardholder claiming:

- He or she was in possession of the valid card on the date of transaction.
- He or she did not authorize or participate in the transaction.

Most Common Causes

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 the entire magnetic stripe.

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 merchant bank with a copy of the printed sales receipt.

Transaction Was Counterfeit

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

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 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.

Key-Entered Transaction

(PM) If you key-enter a transaction because the magnetic stripe cannot be read, be sure to get an imprint of the front of card either on the printed sales receipt or a manual sales receipt form, which should be signed by the customer.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 81: Fraudulent Transaction—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 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.

This chargeback is not valid for recurring payments and card-absent transactions. It is valid for card-present sales on self-serve POS 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.

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 merchant bank 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 merchant bank 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

(PR) If the account number was not obtained from either the magnetic stripe or manually, accept the chargeback.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 81: Fraudulent Transaction—Card-Present Environment (continued)

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 merchant bank. 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.

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. 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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 81: Fraudulent Transaction—Card-Present Environment (continued)

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.

Investigate High Volume of Chargebacks

(PM) If you are receiving a high volume of 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 POS terminals and sales staff were involved in these transactions.

Train Staff to Clean Magnetic-Stripe Readers

(PM) A high volume of 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 merchant bank about point-of-sale training and educational materials and ReaderCleaner™ cards for cleaning magnetic-stripe readers. All are available from Visa.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 83: Fraudulent Transaction—Card-Absent Environment

Definition

The card issuer received:

- A written 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.

Most Common Causes

The merchant:

- Processed a card-absent transaction from a person who was fraudulently using an account number.
- Processed a card-absent transaction without submitting an authorization request.

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 merchant bank 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 merchant bank.

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.*

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 83: Fraudulent Transaction—Card-Absent Environment (continued)

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 merchant bank so it may attempt a representment.

Was a 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 merchant bank 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

(PR) 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.

Identify Transaction as Card-Absent

All card-absent transactions should be identified by the appropriate code for mail order, telephone order, 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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 83: Fraudulent Transaction—Card-Absent Environment (continued)

Owner/Manager

Risk-Management Tools

(PM) For card-absent transactions, consider using AVS, CVV2, and Verified by Visa to help reduce fraud. Contact your merchant bank 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 merchant bank to ensure your merchant name, city, and state, or phone number or Internet address are properly identified in the clearing record.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Authorization Errors

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 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 the card at a POS 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

Most merchant banks 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.

Back-Office Staff

Transaction Was Authorized

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

First Authorization Attempt Declined

(NR) Accept the chargeback if your first authorization attempt was declined. Multiple authorization attempts may not be accepted as valid evidence to show that an approval was obtained.

Point-of-Sale Staff

Obtain Authorization

(PM) Obtain an authorization before completing transactions. With most POS terminals, an authorization request is sent automatically when the card is swiped 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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 71: Declined Authorization (continued)

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, call your voice authorization center. If the transaction is approved, write the approval code on the sales receipt in the appropriate space, and imprint the card's embossed information onto the receipt, using a manual imprinter.

Never Accept a Declined Transaction.

(PM) If a transaction is declined, do not accept it. Immediately stop the transaction, and ask the customer for another Visa card or other form of payment.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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 any of the following:

- Visa Fleet Card $150
- All other cards $75

Most Common Causes

The merchant did not obtain an authorization for a transaction or, for card-present transactions, obtained it after the transaction date.

Merchant Actions

Back-Office Staff

Transaction Was Authorized

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

Most merchant banks 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.

Transaction Was Not Authorized

(NR) Accept the chargeback.

Point-of-Sales Staff

Obtain an Authorization

(PM) Obtain an authorization before completing transactions. The authorization request is sent automatically when you swipe the card and 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 POS terminal.

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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 72: No Authorization (continued)

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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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

Back-Office Staff

Card Not Expired—Key-Entered Transaction

(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 merchant bank. The chargeback is invalid regardless of whether authorization was obtained.

Card Expired, Authorization Obtained

(PR) If the card was swiped or a manual imprint made, and authorization approval was obtained as required, inform your bank of the transaction date and amount. Many merchant banks automatically handle this type of chargeback so you never see it.

Card Expired, No Authorization Obtained

(NR) If the card has expired and you did not obtain an authorization, accept the chargeback.

Point-of-Sale Staff

Check Expiration Date

(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 04/08, the card is valid through April 30, 2008 and expires on May 1, 2008.)

Card-Absent, Authorization Obtained

(PR) If the transaction was a MO/TO or Internet transaction, and authorization approval was obtained/required, inform your bank of the transaction amount and date. Many merchant banks automatically handle this type of chargeback, so you really never see it.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 73: Expired Card (continued)

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 76: Incorrect Transaction Code

Definition

The card issuer received a complaint from a cardholder, stating that a debit was received for a transaction that should have been credited to the account.

Most Common Causes

The merchant issued a credit voucher, but the transaction was posted as a sale.

Merchant Actions

Back-Office Staff

Correct Transaction Code Was Posted

(PR) Provide your merchant bank 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 POS terminal.

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 POS terminals.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 77: Non-Matching Account Number

Definition

The account number transmitted to the card issuer did not match any account number on the card issuer's master file and the transaction was not authorized.

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 merchant bank and request that your bank 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.

Catch-22

After accepting the chargeback, the new transaction with the correct account number should be submitted within 30 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.

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 merchant bank. Request that the bank include the authorization log for this transaction when returning it to the card issuer. Many merchant banks handle this type of chargeback automatically, so that you never receive them.

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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 77: Non-Matching Account Number (continued)

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." 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" (see Glossary). The card issuer may ask you to pick up the card if you can do so safely.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Processing Errors

Reason Code 74: Late Presentment

Definition	The card issuer received a transaction after the 30-day time frame and the account number is blocked or closed.
Most Common Causes	The merchant or service establishment did not deposit the sales receipt with its merchant bank 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 30-day time frame, ask your merchant bank 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 30 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 merchant bank 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 74: Late Presentment (continued)

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 merchant bank.

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. Electronic cash registers 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 80: Incorrect Transaction Amount or Account Number or Invalid Adjustment

Definition

The card issuer identified the transaction amount or the account number posted as being different from what is shown on the sales receipt. For ATM transactions, this error code is used if an adjustment was incorrectly processed.

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 merchant bank to re-present the item.

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.

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), be sure to 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.

Altered Amounts

(PM) Merchants must **not** alter a sales receipt after the cardholder has signed it and left the establishment. If the cardholder has been undercharged, attempt to contact the cardholder and obtain permission to adjust the receipt so that it reflects the correct amount.

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 110).

Invalid Adjustment

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

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 82: Duplicate Processing

Definition

The card issuer received the same transaction more than once for posting to the cardholder's account.

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 merchant bank more than once.
- Deposited with its merchant bank both the merchant copy and the bank copy of a sales receipt.
- Deposited sales receipts for the same transaction with more than one merchant bank.
- Created two sales receipts for the same purchase.

Merchant Actions

Back-Office Staff

Sales Receipts Are Not Duplicates

(PR) Provide your merchant bank 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 merchant bank. 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 merchant bank of the date the credit was issued. If your merchant bank requires other procedures, follow them. However, many merchant banks 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 bank copies—and not merchant copies—are included. If transactions are sent electronically for processing, ensure each batch is sent only once and as a separate batch number.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 82: Duplicate Processing (continued)

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, be sure to 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 86: Paid by Other Means

Definition

The card issuer received a written 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 merchant bank 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 merchant bank with the date of the credit. Many banks 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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

The merchant processed a transaction from:

- A Limited-Amount Terminal and exceeded $25
- A Self-Service Terminal (excluding AFD) and exceeded $50
- An AFD and exceeded:*
  - $150 for Visa Fleet cards
  - $75 for all other cards

Merchant Actions

Back-Office Staff

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

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

Transaction Amount Exceeded $25, $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 merchant bank evidence of the credit.

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.*

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 96: Transaction Exceeds Limited Amount (continued)

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 merchant bank.

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 $85; the card issuer processed a chargeback for $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 merchant bank. 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 merchant bank 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 $25, $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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Cancelled or Returned

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 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 processing the transaction.
- Notified the cardholder in writing within 10 days of processing the recurring transaction, after which the cardholder notified the merchant not to charge the account.

Merchant Actions

Back-Office Staff

Transaction Cancelled and Credit Issued

(PR) If the cardholder claimed to have cancelled the recurring transaction, inform your merchant bank 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 41: Cancelled Recurring Transaction (continued)

Transaction Not Cancelled

(NR) If you have no record that the cardholder cancelled 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 merchant bank 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

If the customer expressly renewed their contract for services, inform your merchant bank.

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 10 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 merchant bank.

Customer Complaints

(CS) (PM) Check customer logs daily for customer complaints, especially those relating to transaction amounts or failure to notify customers in advance of a recurring transaction that exceeds the pre-authorized amount range. Follow up with customers.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 41: Cancelled Recurring Transaction (continued)

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 liable to cardholder disputes.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 53: Not as Described or Defective Merchandise

Definition

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.

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

- Not the same as shown and/or described on-screen (for Internet transactions), or as described on the sales 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).
- Shipped to the cardholder and received, either damaged or defective.

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.
- Merchandise 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.

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 merchant bank 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 merchant bank. (The cardholder must make a valid attempt to return 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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 53: Not as Described or Defective Merchandise (continued)

Back-Office Staff

Merchandise Was As Described

(PR) If the merchandise was as described, provide your merchant bank 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 merchant bank 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.

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.

Card issuer Waiting Period. If merchandise was returned, the card issuer must wait at least 30 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.

Quality Disputes. This chargeback 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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 merchant bank in time for it to appear on the cardholder's next statement.
- Did not issue a credit because the business does not accept returns (but the merchant did not properly disclose its return policy).

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 merchant bank 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 merchant bank 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.

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 merchant bank 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 merchant bank of the date that the credit was issued.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 85: Credit Not Processed (continued)

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.

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 merchant bank showing that the credit was given to the gift recipient.

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.

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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 85: Credit Not Processed (continued)

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. For Internet transactions, your website should include a screen that appears automatically during the check-out process (that is, not on a separate disclosure screen that the customer has to click to open) informing customers of your return or refund policies. The screen should include **"Accept"** or **"Agree"** buttons for the customer to click on before completing the transaction, indicating that he or she has read and agreed to your policies.

*If a cardholder can complete an Internet transaction without clicking an **"Accept"** or **"Agree"** button to indicate acceptance of your refund, return, or cancellation policy, proper and adequate disclosure has not occurred.*

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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Non-Receipt of Goods or Services

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 merchant bank with details of the delivery or send your merchant bank 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 merchant bank that the software was downloaded to or received by the cardholder.

Less Than 30 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 30 days from the transaction date, send a copy of the sales receipt to your merchant bank pointing out that 30 days have not yet elapsed. You should also state the expected delivery date.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 30: Services Not Provided or Merchandise Not Received (continued)

Specified Delivery Date Has Not Yet Passed

(PR) If the specified delivery date has not yet passed, return the chargeback to your merchant bank 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.

Merchandise Shipped After Specified Delivery Date

(PR) If the merchandise was shipped after the specified delivery date, provide your merchant bank 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 merchant bank 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 merchant bank: 1) the merchandise was available for the cardholder to pick up, 2) the chargeback was processed less than 30 days from the transaction date and no pick up date was specified, 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.

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.

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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Reason Code 30: Services Not Provided or Merchandise Not Received (continued)

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 merchant bank 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

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

APPENDIX 1 Training Your Troops

What's Covered

- Training Materials for Card-Present Merchants
- Training Materials for Card-Absent Merchants
- Training Materials on Cardholder Information Security Program (CISP)

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

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

- Sales 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 have fewer fraudulent transactions, which reduces related losses.
  - You have fewer transaction receipt copy requests and chargebacks, which reduces related expenses.

The Visa resources listed in this section can be used to help educate your sales and customer service associates and bring them up to speed on all the latest procedures.

To order any of the training materials listed in this chapter, call Visa Fulfillment at (800) VISA-311 or visit *www.visa.com/merchant*.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Training Materials for Card-Present Merchants

Point-of-Sale Reminder Card

Designed for use at the point of sale, this six-panel card helps sales staff remember the correct steps for accepting and processing Visa cards.

Price: $0.25 each *VRM 09.08.07*

It Pays to Swipe the Stripe

Designed for both merchants and point-of-sale staff, this brochure includes quick and easy tips to ensure proper use of magnetic-stripe readers. It also covers the basics of key entry and what to do when a magnetic stripe can't be read.

Price: $0.25 each *VRM 10.02.05*

Improve Profitability: Eliminate Illegible Sales Drafts

This six-panel brochure outlines the reasons why sales drafts must be readable and provides tips on how to make sure customer transactions can be tracked. It is designed for use at the point of sale or for posting in training areas, lunchrooms, or wherever your sales staff can see it as a quick reminder.

Price: $0.25 each *VRM 04.25.07*

Visa Pin Security Tools and Best Practices for Merchants

Visa Pin Security Tools and Best Practices for Merchants provides an overview of Visa's initiatives and requirements, circumstances that lead to PIN vulnerabilities, and best practices to avoid PIN and data theft.

Price: Free *VRM 08.05.07*

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Card Acceptance and Fraud Awareness for Merchants: "Fraud Factor"

This lively, entertaining video describes card-acceptance procedures for retail merchants. It also reviews card security features and outlines what to do when something about the transaction raises suspicions.

Price: $3.00 *VRM 08.17.06*

Visa's How-To For Restaurant Owners and Managers

This four-page brochure offers best practices to help restaurant merchants prevent both fraud and chargebacks. Topics covered range from merchant set-up and zero-percent tip authorization to skimming and chargeback management.

Price: Free *VRM 01.22.07*

Visa Tips for Restaurant Staff

The Visa Tips for Restaurant Staff is an invaluable tool for employees who are responsible for processing card transactions. Designed for ease of use, the on-the-job reference brings together practical information and practices to ensure proper payment acceptance, minimize fraud exposure, and reinforce 0% tip authorization requirements

Price: Free *VRM 08.15.06*

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Training Materials for Card-Absent Merchants

E-Commerce Merchants' Guide to Risk Management

This 106-page book features risk management best practices for selling goods and services on the Internet. It covers a range of topics including e-commerce start-up, website utility, fraud prevention, Visa card acceptance, cardholder information security, and chargeback handling and loss recovery.

Price: $2.00 each *VRM 08.01.08*

Visa Card Verification Value 2 (CVV2) Merchant Guide

This four-page brochure provides a detailed look at the CVV2 process. It includes instructions on how to use CVV2 to maximize security and protect against fraud.

Price: Free *VRM 03.14.06*

Merchant Guide to Visa Address Verification Service (AVS)

This 16-page guide describes AVS, Visa's risk management service for card-absent transactions. Targeted at MO/TO and Internet merchants, the guide explains how to maximize the fraud-reduction benefits of AVS and also covers recent system enhancements and dial-up access.

Price: $0.25 each *VRM 01.01.06*

Protect Your E-Commerce Channel Against Fraud

This three-fold brochure is a fast and easy reference for Internet merchants. It contains best practices to help prevent fraud and fraud-related losses for online transactions.

Price: $5.00 for 100 *VRM 03.15.07*

Merchant Best Practices for Recurring Transactions

This brochure contains merchant tools and best practices for effectively handling recurring transactions. Step-by-step procedures cover all aspects of the recurring-transaction life cycle, from initial setup to handling customer-dispute chargebacks.

Price: Free *VRM 03.03.06*

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Training Materials on Cardholder Information Security Program (CISP)

Visa Cardholder Information Security Program CISP Overview

Intended for use as a quick reference, this flyer contains the "Digital Dozen," the 12 security standards required for CISP compliance.

Price: Free *VRM 08.30.06*

Just Another Day at the Office

This 10-minute video uses a comic approach to highlight the administrative and physical issues that are critical for protecting cardholder data.

Price: $3.00 video/DVD *VBS 12.01.00*

Additional Resources

Visa Merchant Catalog – Education, Tools, and Materials

This catalog contains a comprehensive list of all currently available Visa training materials.

Price: Free *VRM 09.01.08*

Visa USA website (www.visa.com/merchant)

This website links to a comprehensive range of products and services for Visa merchants.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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.

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,: *Voice Authorization Center*.

"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 "Good Thru" 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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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 *Visa U.S.A. Inc. Operating Regulations*. Card-present merchants must check these features when processing a transaction at the point of sale to ensure that a card is valid.

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.

Cardholder Information Security Program (CISP)
A Visa program that establishes data security standards, procedures, and tools for all entities (merchants, service providers, issuers, and merchant banks) that store Visa cardholder account information. CISP compliance is mandatory.

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 a merchant bank by a card issuer, usually because of a disputed transaction. The merchant bank may then return or "charge back" the transaction to the merchant.

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 a merchant bank for a copy or facsimile of a sales receipt for a disputed transaction. Depending on where sales receipts are stored, the merchant bank either fulfills the copy request itself or forwards it to the merchant for fulfillment. A copy request is also known as a retrieval request.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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.

"Doing Business As" (DBA)
A merchant's legal business name as differentiated from the names of a company's principals or other entity that owns or manages the business. A DBA that is significantly different from the principals' or other entity's name can result in an unrecognizable merchant name, or descriptor, on a cardholder's monthly Visa statement, which can lead to potential copy requests and chargebacks.

Dynamic Currency Conversion (DCC) Service
An optional service, that is facilitated by a merchant at the point of sale with either a third party agent or through its merchant bank. The DCC allows a cardholder to see the transaction amount in his or her billing currency **and** the merchant's pricing currency. This way, the cardholder knows exactly how much the goods or services cost and is able to make value judgments quickly and easily.

Electron card
A debit or prepaid card that is issued in countries around the world. The card is currently not issued in the United States 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.

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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

"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 transaction is valid. See also, *Card expiration date*.

High-Risk Chargeback Monitoring Program (HRCMP)
A Visa program that notifies merchant banks when a high-risk merchant has a chargeback-to-transaction rate of over one percent.

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, High-Risk Chargeback Monitoring Program.

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.

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 *Visa U.S.A. Inc. Operating Regulations.* The stripe is "read" when a card is swiped through a POS 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. Such transactions are frequently charged to customers' bankcard accounts. See also, *Card-absent*.

Member
An organization that is a member of Visa and issues cards and/or signs merchants.

Merchant agreement
The contract between a merchant and a merchant bank 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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Merchant bank
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.

Merchant Chargeback Monitoring Program (MCMP)
A Visa program that alerts merchant banks when one of their merchants has a chargeback-to-transaction rate of over one percent. Merchants then work with the bank 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.

Payment gateway
A system that provides services to Internet merchants for the authorization and clearing of online Visa transactions.

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 terminal (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 *Visa U.S.A. Inc. Operating Regulations* refers to the three types of processors: authorizing processors, clearing processors, and V.I.P. system users. See also, *VisaNet processor*.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

Representment
A chargeback that is rejected and returned to a card issuer by a merchant bank on the merchant's behalf. A chargeback may be re-presented, or redeposited, if the merchant or merchant bank can remedy the problem that led to the chargeback. To be valid, a representment must be in accordance with *Visa U.S.A. Inc. Operating Regulations.*

Sales receipt
The paper or electronic record of a bankcard transaction that a merchant submits to a merchant bank for processing and payment. In most cases, paper drafts are now generated by a merchant's POS 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 (TPA)
Is an entity that is not defined as a VisaNet Processor, but instead provides payment related services, directly or indirectly, to a member and/or stores, processes, or transmits cardholder data. TPAs must be registered by all Visa members that are 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 issuers and merchant banks.

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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

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 ReaderCleaner™

A specially treated card that effectively removes dirt, magnetic oxides, and other contaminants from concealed magnetic heads in POS devices. The heads should be kept clean so that Visa cards can be swiped and their magnetic stripes read quickly and easily, thus avoiding key-entered transactions.

VisaNet processor

A processor directly connected to VisaNet. See also, *Processor*.

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 POS 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.

©2008 Visa Inc., all rights reserved, to be used solely for the purpose of providing Visa Card acceptance services as authorized pursuant to agreement with a Visa member financial institution.

© 2008 Visa U.S.A. Inc. VRM 07.31.08