# Card Acceptance Guidelines for Visa Merchants

© 2011 Visa. All Rights Reserved.

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Section 1: Getting Down to Basics</strong></td>
<td>5</td>
</tr>
<tr>
<td>Visa Transaction Processing—Who is Involved?</td>
<td>6</td>
</tr>
<tr>
<td>Visa Transaction Flow for Magnetic-Stripe and Chip Cards</td>
<td>7</td>
</tr>
<tr>
<td>Visa Transaction Flow for PIN-Based Point-of-Sale and ATM</td>
<td>9</td>
</tr>
<tr>
<td>Visa Rules</td>
<td>11</td>
</tr>
<tr>
<td>Visa Rules for Returns and Exchanges</td>
<td>16</td>
</tr>
<tr>
<td>Visa Rules for PIN-less Payment Brand Acceptance (U.S. Only)</td>
<td>18</td>
</tr>
<tr>
<td><strong>Section 2: Card-Present Transactions</strong></td>
<td>19</td>
</tr>
<tr>
<td>Doing It Right at the Point of Sale</td>
<td>20</td>
</tr>
<tr>
<td>Visa Card Features and Security Elements</td>
<td>25</td>
</tr>
<tr>
<td>Authorization</td>
<td>29</td>
</tr>
<tr>
<td>Cardholder Verification and Identification</td>
<td>32</td>
</tr>
<tr>
<td>Suspicious Behavior</td>
<td>35</td>
</tr>
<tr>
<td>Skimming</td>
<td>36</td>
</tr>
<tr>
<td>Code 10 Calls</td>
<td>37</td>
</tr>
<tr>
<td>Recovered Cards</td>
<td>38</td>
</tr>
<tr>
<td>Visa payWave Transactions</td>
<td>39</td>
</tr>
<tr>
<td>Visa Easy Payment Service Transactions</td>
<td>40</td>
</tr>
<tr>
<td>Electron Cards</td>
<td>42</td>
</tr>
<tr>
<td>Visa Travelers Cheques</td>
<td>43</td>
</tr>
<tr>
<td><strong>Section 3: Card-Absent Transactions</strong></td>
<td>45</td>
</tr>
<tr>
<td>General Card-Absent Transaction Procedures</td>
<td>46</td>
</tr>
<tr>
<td>Fraud Prevention Guidelines for Card-Absent Transactions</td>
<td>47</td>
</tr>
<tr>
<td>Additional Fraud Prevention Tools for the Internet</td>
<td>55</td>
</tr>
<tr>
<td>Suspicious Transactions</td>
<td>60</td>
</tr>
<tr>
<td>Recurring Transactions</td>
<td>63</td>
</tr>
<tr>
<td><strong>Section 4: Payment Card Industry Data Security Standard and PIN Security and Key Management</strong></td>
<td>67</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard Requirements</td>
<td>68</td>
</tr>
<tr>
<td>Visa PIN Security and Key Management Compliance Program</td>
<td>71</td>
</tr>
</tbody>
</table>
Introduction

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

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

Contents
The Card Acceptance 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 (AVS)* 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—Comprehensive coverage of the Payment Card Industry and Data Security Standard (PCI DSS) requirements, with which all merchants and service providers must comply, to help ensure the security of confidential cardholder information. PCI PIN Security Requirements are also discussed.

✔ Appendix 1: Training Your Staff A reference to Visa.com which offers resources that merchants can use for training their employees on card acceptance and fraud prevention procedures.

✔ Appendix 2: Glossary—A list of terms used in the guide.

✔ Appendix 3: Visa Europe Territory—A list of Visa European Territories.

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

** In certain markets, CVV2 is required to be present for all card-absent transactions.
Most of the information and best practices contained in this document pertain to all regions; however in some countries, there are specific products, services, and regulatory differences that must be noted. In these instances, country or region-specific details have been identified with a universally recognized icon for the country under discussion.

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

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

The country icons are as follows:

- 🇺🇸 United States
- 🇨🇦 Canada
- 🇧🇷 Latin America and Caribbean (LAC)
- 🇦🇺 Asia Pacific (AP)
- 🇧🇪 Central Europe, Middle East, and Africa (CEMEA)

The Card Acceptance Guidelines for Visa Merchants provides icons that highlight additional resources or information:

<table>
<thead>
<tr>
<th>Icon:</th>
<th>Definition:</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔍</td>
<td>Additional insights related to the topic that is being covered.</td>
</tr>
<tr>
<td>🗂️</td>
<td>A brief explanation of additional Visa resources that are pertinent to the topic at hand.</td>
</tr>
</tbody>
</table>
The information in this guide is current as of the date of printing. However, card acceptance and processing procedures are subject to change. This guide contains information based on the current Visa International Operating Regulations. If there are any differences between the Visa International Operating Regulations and this guide, the Visa International Operating Regulations will prevail in every instance. Your merchant agreement and the Visa International Operating Regulations take precedence over this guide or any updates to its information. To access a copy of the Visa International Operating Regulations, visit www.visa.com/merchant and click on Operations and Procedures.

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

The information, recommendations or “best practices” contained in this guide are provided “AS IS” and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. This guide does not provide legal advice, analysis or opinion. Your institution should consult its own legal counsel to ensure that any action taken based on the information in this guide is in full compliance with all applicable laws, regulations and other legal requirements.

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

For further information about the rules or practices covered in this guide, contact your acquirer.
Introduction
Getting Down to Basics

What’s Covered

- Visa Transaction Processing—Who is Involved?
- Visa Transaction Flow for Magnetic-Stripe and Chip Cards
- Visa Transaction Flow for PIN-Based Point-of-Sale and ATM
- Visa Rules
- Visa Rules for Returns and Exchanges
- Visa Rules for PIN-less Payment Brand Acceptance

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

Parties to Visa Transactions

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

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

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

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

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

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

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

- An authorization service through which card issuers can approve or decline individual Visa card transactions.

- A clearing and settlement service that processes transactions electronically between acquirers and card issuers to ensure that:
  - Visa transaction information moves from acquirers to card issuers for posting to cardholders’ accounts.
  - Payment for Visa transactions moves from card issuers to acquirers to be credited to the merchant accounts.
Visa Transaction Flow for Magnetic-Stripe and Chip Cards

Transaction Life Cycles

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

**Magnetic-Stripe and Chip Card—Credit or Debit Authorization**

**Merchant** or cardholder swipes the card through a magnetic-card reader, dips the card into a chip-reading device,** or waves the card in front of a Visa payWave reader.

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 Card Verification Value 2 (CVV2).*

Merchant enters the transaction amount, and, if necessary, transmits an authorization request to the acquirer.** For card-absent transactions, the account number and other information may be digitally or key-entered.

Acquirer electronically sends the authorization request to VisaNet.

VisaNet passes on the request to the card issuer.

Card issuer provides an online response.

Before approving a transaction, the issuer may check to make sure the cardholder has available funds for credit, then:

- Checks the exception file for all “statused” accounts such as lost, stolen, counterfeit, and credit problems.
- Applies risk-based rules or parameters, such as velocity checks, or a neural network to minimize fraudulent transactions.

If a match is made, the transaction is declined and a response is given to the merchant which could include instructions to retain the card.

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

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

*** In some markets, chip and Visa payWave allow for chip-based offline authorization.
Magnetic-Stripe and Chip Card—Clearing and Settlement

**Acquirer** credits the merchant’s account and electronically submits the transaction to Visa for settlement.

**Merchant** deposits the transaction receipt with acquirer.*

**VisaNet:**
- Facilitates settlement.
- Pays the acquirer and obtains settlement from the card issuer then sends the transaction to the card issuer.

**Card issuer:**
- Posts the transaction to the cardholder account.
- Sends the monthly statement to the cardholder.

**Cardholder** receives the statement.

---

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

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

**Interlink Authorization, Clearing and Settlement**

*Many Visa cards have a chip that communicates information to a point-of-sale terminal with a chip-reading device,* or waves the card in front of a Visa payWave reader. The merchant then enters the transaction amount. The cardholder enters the PIN. A transaction authorization request is transmitted to the acquirer.

**Merchant** or cardholder swipes the card through a magnetic-card reader, dips the card into a chip-reading device,* or waves the card in front of a Visa payWave reader. The merchant then enters the transaction amount. The cardholder enters the PIN. A transaction authorization request is transmitted to the acquirer.

**Acquirer gateway** or acquirer back office determines the network to which the transaction should be routed.

For Interlink, the acquirer gateway or acquirer back office electronically sends the authorization request to VisaNet. All other transactions are transmitted to the appropriate network.

**Other networks**

**VisaNet**

• Passes on the request to the card issuer.
• Facilitates settlement.

**Card issuer**

• Provides an online response.
• Posts the transaction to the cardholder account.

Before approving a transaction, the issuer may check to make sure the cardholder has available funds or credit, then:

- Checks for all “statused” accounts such as lost, stolen, and counterfeit.
- Validates the PIN.

**Acquirer** forwards the response to the merchant.

**VisaNet** forwards the card issuer’s authorization response to the acquirer.

**Merchant** receives the authorization response and completes the transaction accordingly.
Section 1: Getting Down to Basics

Visa/Plus Authorization, Clearing and Settlement

1. Cardholder presents Visa card at ATM, enters PIN, and makes cash withdrawal request.

2. The ATM acquiring bank routes the cash withdrawal authorization request based on ATM network processing preferences.

3. On-Us (Acquirer is also the card issuer)
   - Visa/Plus forwards the card issuer's response to the ATM acquiring bank.
   - Visa/Plus
     - Passes on the request to the card issuer.
     - Facilitates settlement.

4. Card issuer
   - Provides an online response.
   - Posts the transaction to the cardholder account.

5. Other networks

6. ATM dispenses cash to cardholder.

Before approving a transaction, the issuer may check to make sure the cardholder has available funds, then:
- Checks for all “statused” accounts such as lost, stolen and counterfeit.
- Validates the PIN.
Visa Rules

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

Taxes

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

Card Acceptance

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

Minimum/Maximum Purchase

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

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

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

No Surcharging

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

Prohibited Uses

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

Quick Tip

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

* Visa debit and credit cards may have different acceptance policies if you are located in the U.S., Australia, or Canada.
** There are certain variations of the “No Surcharging” rule, depending on local law and acquiring practices. Check with your acquirer regarding prohibited surcharges and/or discounts.
Section 1: Getting Down to Basics

## Convenience Fees*

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

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

## Laundering

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

## Zero-Percent Tip

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

Cardholders now have the ability to check their credit or checking accounts almost instantaneously via phone, the Internet, or an ATM. An authorization that includes an estimated tip can reduce a cardholder’s available funds or credit by an unrecognizable or unexpected amount. This kind of transaction may occur if a cardholder leaves a cash tip or adds a tip that is less than the estimated amount used for authorization. For example, a restaurant authorizes for an estimated 20 percent tip, but the customer adds on only 15 percent.

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

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

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

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

---

* Visa Convenience Fees are permitted only under certain circumstances in the U.S., CEMEA, and Asia Pacific.
Section 1: Getting Down to Basics

No Cash Refunds

Complete a Visa credit receipt for merchandise returns or adjustments. Do not provide cash refunds for returned merchandise originally purchased with a Visa card. Visa does not permit cash refunds for any credit or debit card transaction. By issuing credits, you protect your customers from individuals who might fraudulently make a purchase on their Visa account and then return the merchandise for cash.

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

Deposit Time Limits

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

Suppressed Account Number and Expiration Date

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

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

Delivery of Goods and Services

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

Delayed Delivery

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

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

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

### Installment Payments

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

### Cardholder Information

*Keep cardholder account numbers and personal information confidential.* Cardholders **expect** you to safeguard any personal or financial information they may give you in the course of a transaction. Keeping that trust is essential to fraud reduction and good customer service. Cardholder account numbers and other personal information should be released only to your acquirer or processor, or as specifically required by law.

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

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](#).
Merchant Servicer Registration

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

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

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

For more information on Visa’s data security requirements and programs, see Section 4, Payment Card Industry Data Security Standard and PIN Security and Key Management.

Sensitive Data Storage and Payment Application Use

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

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

* In certain markets, CVV2 is required to be present for all card-absent transactions.
Visa Rules for Returns and Exchanges

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

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

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.

<table>
<thead>
<tr>
<th>Disclosure Statement</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Refunds or Returns or Exchanges</td>
<td>Your establishment does not issue refunds and does not accept returned merchandise or merchandise exchanges.</td>
</tr>
<tr>
<td>Exchange Only</td>
<td>Your establishment is willing to exchange returned merchandise for similar merchandise that is equal in price to the amount of the original transaction.</td>
</tr>
<tr>
<td>In-Store Credit Only</td>
<td>Your establishment takes returned merchandise and gives the cardholder an in-store credit for the value of the returned merchandise.</td>
</tr>
<tr>
<td>Special Circumstances</td>
<td>You and the cardholder have agreed to special terms (such as late delivery charges or restocking fees). The agreed-upon terms must be written on the transaction receipt or a related document (e.g., an invoice). The cardholder’s signature on the receipt or invoice indicates acceptance of the agreed-upon terms.</td>
</tr>
<tr>
<td>Timeshare</td>
<td>You must provide a full credit when a transaction receipt has been processed and the cardholder has cancelled the transaction within 10 calendar days of the transaction date.</td>
</tr>
</tbody>
</table>
Section 1: Getting Down to Basics

Disclosure for Card-Absent Merchants

**Mail Order**

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

**Internet**

Your website must communicate its refund policy to the cardholder and require the cardholder to select a “click-to-accept” or other affirmative button to acknowledge the policy. The terms and conditions of the purchase must be displayed on the same screen view as the checkout screen that presents the total purchase amount, or within the sequence of website pages the cardholder accesses during the checkout process.
Visa Rules for PIN-less Payment Brand Acceptance (U.S. Only)

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

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 clearer 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 expressly 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).
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 may 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.
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 following illustrations provide an overview of the card acceptance steps that should be followed at a point-of-sale terminal. Each step is explained in greater detail in this section.

Illustration of Card Acceptance (Magnetic Stripe Card Processing)

Swipe the card through a magnetic card reader or wave the card in front of a Visa payWave contactless reader to request the transaction authorization.

While the transaction is being processed, check the card’s features and security elements, if possible. Make sure the card is valid and has not been altered in any way.

Obtain authorization and, if required, get the cardholder signature* on the transaction receipt.

Compare the name, number, and signature* on the card to those on the transaction receipt.

If you suspect fraud, make a Code 10 call.

For more information about making a Code 10 call, please refer to page 37 in this guide.

* The cardholder signature is not required if the transaction is PIN-Verified, processed with Visa Easy Pay Service (VEPS), or with some Visa payWave transactions.
Illustration of Card Acceptance (Chip Card Processing)

In simple terms, a chip card is a plastic payment card with an embedded computer chip containing a microcomputer, analogous to a personal computer with memory. Chip cards offer a variety of benefits such as:

- Extremely difficult to copy
- Facilitates the evolution of security methods and processes
- Capability of holding many applications
- Keeps and updates large amounts of data
- Enhanced options to support PIN
- Performs calculations and makes decisions
- Enhances confidence in the payments system

The card and chip-reading device work together to determine the appropriate cardholder or verification method for the transaction either signature, PIN, or Visa EasyPay Service (VEPS).

If the transaction requires a PIN-verification, the cardholder follows point-of-sale prompts and enters the PIN. There is no opportunity to examine the card. It is retrieved by the cardholder.

If you suspect fraud, make a Code 10 call.

The merchant prints a copy of transaction receipt for cardholder. If the transaction is not PIN-based, the receipt will have a signature line. The merchant must ask the cardholder to sign the receipt.

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

** Some chip-reading devices support a “merchant suspicious” indicator on the authorization.
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.

Always Dip the Chip

When the Visa card that is being presented has a chip and the merchant has a point-of-sale terminal with a chip-reading device, follow these steps.

- **Insert the chip card into the chip-reading device.**
  - Make sure your staff or the cardholder inserts the card into the chip-reading device. If the card is swiped first, the terminal will read the service code and prompt you to insert the card into the chip-reading device.
  - Follow the picture or diagram displayed on the terminal screen that shows which way the chip should face.
  - Keep the card inserted in the chip-reading device during the entire transaction (do not swipe the card unless the terminal screen instructs you to).
  - Do not remove the card until you are instructed to do so by the chip-reading device.

- **Follow the instructions on the terminal screen.** The chip-reading device compares the applications it supports to the applications available on the card, then displays instructions on how to proceed.
  - If the card and chip-reading device have one application in common, that application is automatically used.
  - If the card and chip-reading device have more than one application in common, the terminal screen may display a list of applications to the cardholder.
  - If the chip-reading device cannot read the chip on the card, it means the card and chip-reading device have no applications in common. In this case, you should follow “fallback” requirements and accept the chip card via standard magnetic stripe transaction processing as prompted on the terminal screen.

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

- **Always make sure that the chip-reading device is easily accessible to the cardholder.**

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

- The terminal's magnetic-stripe reader is not working properly.
- The card is not being swiped through the reader correctly.
- You may have a counterfeit or altered payment card.
- 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 in this section.)
- 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 can protect 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.
- If an unembossed card will not swipe, you should ask for another form of payment. Do not manually key enter unembossed cards, or write the account number on a paper draft. A marked paper draft will not protect merchant against chargeback.

For some merchants, a high key entry rate is due to misclassification of card-absent transactions so they look like card-present transactions. Consult with your acquirer to make sure your card-absent transactions are correctly classified with accurate MO/TO and ECI indicators.

If the Terminal Cannot Read the Chip

When normal chip transactions cannot be processed at chip terminals, the merchant “falls back” to lesser method. Because the fallback transaction is swiped or keyed, the normal rules of transaction processing for magnetic stripe or key entry as applicable will come into play. This means that a signature will be required, rather than a PIN. For key-entered transactions, manual imprints will be required.
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 Fallback 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.

**Find Causes and Look for Solutions**

If your key-entry or fallback 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.

<table>
<thead>
<tr>
<th>Key-Entry Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damaged Magnetic-Stripe Readers or Chip-Reading Device</td>
<td>Check magnetic-stripe readers or chip-reading devices regularly to make sure they are working.</td>
</tr>
<tr>
<td>Dirty Magnetic-Stripe Readers or Chip-Reading Device</td>
<td>Clean magnetic-stripe reader or chip reading device heads several times a year to ensure continued good use. Follow the cleaning instructions supplied with the terminal.</td>
</tr>
<tr>
<td>Magnetic-Stripe Reader or Chip-Reading Device Obstructions</td>
<td>Remove obstructions near the magnetic-stripe reader or chip-reading device. Electric cords or other equipment could prevent a card from being swiped straight through the reader in one easy movement.</td>
</tr>
<tr>
<td>Spilled Food or Drink</td>
<td>Remove any food or beverages near the magnetic-stripe reader or chip-reading device. Falling crumbs or an unexpected spill could soil or damage the machine.</td>
</tr>
<tr>
<td>Anti-Theft Devices that Damage Magnetic Stripes</td>
<td>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.</td>
</tr>
<tr>
<td>Improper Card Swiping</td>
<td>• Swipe the card in one quick, smooth motion.</td>
</tr>
<tr>
<td></td>
<td>• Never swipe a card back and forth.</td>
</tr>
<tr>
<td></td>
<td>• Never swipe a card at an angle. This may cause a faulty reading.</td>
</tr>
<tr>
<td>Improper Card Dipping</td>
<td>• Dip the card in one quick, smooth motion.</td>
</tr>
<tr>
<td></td>
<td>• Never dip a card in and out.</td>
</tr>
<tr>
<td></td>
<td>• Never dip a card at an angle: Leave the chip card in the reading device until instructed to remove it.</td>
</tr>
</tbody>
</table>
Card Acceptance Guidelines for Visa Merchants

Section 2: Card-Present Transactions

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.

What to Look for on all Visa Cards

Visa Brand Mark Card Security Features

The **Signature Panel** must appear on the back of the card and contain an ultraviolet element that repeats the word “Visa®.” The panel will look like this one, or have a custom design. It may vary in length.

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

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

The **Magnetic Stripe** is encoded with the card’s identifying information.

**Card Verification Value (CVV)** is a unique three-digit code that is encoded on the magnetic stripe of all valid cards. CVV is used to detect a counterfeit card.

**Card Verification Value 2 (CVV2)** is a three-digit code that appears either in a white box to the right of the signature panel, or in a white box within 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 customer is in possession of a valid Visa card at the time of the sale.

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

If you do not see a mini-dove on the back of the card, check for the traditional dove hologram above the Visa Brand Mark on the front of the card.

**Expiration or “Good Thru” date** should appear below the account number.

**Cardholder Name or a Generic Title** may be embossed or printed on the card. This field may be blank on some Visa cards.

**Embossed/Unembossed or Printed Account Number** on valid cards begins with “4.” All digits must be even, straight, and the same size.

**Four-Digit Bank Identification Number (BIN)** must be printed directly below the account number. This number must match exactly with the first four digits of the account number.

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

* In certain markets, CVV2 is required to be present for all card-absent transactions.
## Alternative Visa Brand Mark Applications

The two-color Visa Brand Mark (as shown here) does not have the standardized white background.

The two-color reverse Visa Brand Mark (as shown here) does not have the standardized white background and has been reversed to white with a gold wing within the letter form of the V.

---

## Visa Mini-Card

A Visa Mini Card is a miniature version of a standard size Visa Card or Visa Electron Card.

---

## Visa Vertical Card

This card has a vertical orientation and account information is laser printed on the card, not embossed. It includes a magnetic stripe just like its embossed counterpart, and a card verification code on the back.
Section 2: Card-Present Transactions

Unembossed Visa Card Acceptance

The unembossed Visa card (e.g., prepaid card) may look and feel different, but it is a valid card that can be accepted at any Visa merchant location that has an electronic terminal. Unlike an embossed Visa card with raised numbers, letters, and symbols, the unembossed card has a smooth, flat surface. From a merchant perspective, the processing of an unembossed card at the point-of-sale should be seamless. There’s no need for new software, special hardware, or modified terminal procedures. You simply swipe the unembossed card just as you would an embossed card, then wait for an authorization and obtain the cardholder’s signature. Because of the unembossed card’s flat surface, it cannot be used for transactions that require a card manual imprint. Merchant should not attempt to hand-write receipts or key-enter the account number for unembossed cards.

Full Magnetic-Stripe Data must be transmitted as part of the unembossed Visa card transaction authorization. Merchants are required to swipe an unembossed card through the terminal to prove that the card was present at the time of the transaction.

Unembossed 16-digit Account Number, Cardholder Name, and Expiration Date are laser-engraved, thermal or indent-printed securely on the front of the card. The card’s flat, smooth surface makes it impossible to take a manual imprint. If the Dove Hologram is on the front of the card, the account number will be printed outside the hologram. The numbers may be smaller and placed closer together.

Cardholder Name or a Generic Title may appear on an unembossed card. This field may be blank on some Visa cards.

Visa Chip Card

Visa Chip cards are embedded with a chip that communicates information to a point-of-sale terminal.
Visa Electron Card*

Visa Electron cards feel flat; all information is printed or engraved, not embossed or raised. Some unembossed Visa cards may have only a partial account number printed on the card. The Visa Dove Design Hologram may or may not appear on Visa Electron cards. This field may be blank on some Visa Electron cards.

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 37 of this document.)

* Visa Electron Card is only available in certain countries, but is accepted worldwide.
Section 2: Card-Present Transactions

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 helps protect 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).

<table>
<thead>
<tr>
<th>Response</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>Card issuer approves the transaction. This is the most common response.</td>
</tr>
<tr>
<td>Declined or Card Not Accepted</td>
<td>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.</td>
</tr>
<tr>
<td>Call, Call Center, or Referrals</td>
<td>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.</td>
</tr>
<tr>
<td>Pick Up</td>
<td>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 Recovered Cards on page 38 of this document).</td>
</tr>
</tbody>
</table>

When a transaction is approved, the point-of-sale terminal automatically prints a sales receipt. When a negative or alert message is received, the response is displayed on the point-of-sale 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.

Authorization should be seen as an indication that account funds or credit is available and the card has not been reported as lost or stolen.

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.
Handling Authorizations

Below the Floor Limit

For “below-floor-limit” transactions the merchant has the option to do the following:

- For magnetic-stripe card transactions, seek authorization
- For chip card transactions, either obtain offline approval or seek online authorization
- Not seek the authorization, but compare the card number to the current Card Recovery Bulletin (CRB). **This action is no longer a requirement for merchants using chip terminals in some Visa regions. Check with your Visa representative to confirm the status in your location.**

If the merchant is presented with a card that is listed on the CRB, the merchant must:

- Not complete the transaction.
- Retain the card by reasonable, peaceful means, if safe to do so. **Do not put yourself at risk.**
- Call the authorization center, state that the card number is on the bulletin, give the account number, and ask for instructions.

If the card number is not on the bulletin and the transaction amount is below the merchant floor limit, it is not mandatory for the merchant to obtain an online authorization. The merchant may proceed with the transaction. There are, however, some exceptions to this rule.

A merchant must obtain an online authorization for manual cash, Electron card, expired card, or unattended terminal transactions, and for fallback transactions (when the chip card cannot read at a chip terminal) or if the chip card requests the terminal to proceed with an online authorization.

**Note:** The embedded chip on the card contains issuer-defined parameters that guide the acceptance procedure in a full chip transaction. The chip can be programmed to request that a chip-enabled terminal proceed with an online authorization, or communicate that a transaction be authorized offline by the chip.

For some merchants in other countries, the floor limit is zero, in this case merchants must obtain an authorization for all transactions.

The Card Recovery Bulletin (CRB) is an international list of lost/stolen, counterfeit, and other cards that card issuers have listed for pickup.
Section 2: Card-Present Transactions

Zero-Percent Tip Authorizations

See page 12 in this guide for further details.

Split-Tender Transactions

A split-tender transaction occurs when a cardholder purchases goods or services in part with a Visa card and in part with 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.

If you do accept split-tender transactions, and the total amount exceeds the Visa floor limits, authorization for the Visa part of the transaction must be obtained—even if the amount being paid is below your floor limit.

Partial Authorizations

Partial Authorization provides an alternative to a declined transaction by permitting a 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 available balance on the Visa card and select another form of payment (e.g., another payment card, cash, check) for the remaining amount transaction. Partial Authorization can benefit all stakeholders, resulting in improved cardholder satisfaction at the point-of-sale and increased sales. For further information on Partial Authorizations, contact your acquirer.
Cardholder Verification and Identification

The final step in the card acceptance process for transactions requiring a signature is to ensure that the customer signs the sales receipt and to compare that signature with the signature on the back of the card. Depending on the Visa card product and point-of-sale terminal processing system, the customer should be in full view when signing the receipt or point-of-sale terminal signature window display. If possible, you should check the two signatures closely for any obvious inconsistencies in spelling or handwriting.

Checking Signatures

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

- For magnetic-stripe card transactions, match the name and last four digits of the account number on the card to those printed on the receipt.

- When a signature has been obtained, 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.

When a Signature Line is Not Present

When a magnetic-stripe or chip card transaction is PIN-based and the merchant has an active PIN pad, Visa's best practice is not to print a signature line on the receipt. Merchants need to be aware that they should not request a signature from the cardholder when a signature line is not present on the receipt.
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.

“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 often 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.

In this situation, follow recommended steps listed above under Unsigned Cards.
**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 except in the specific circumstances discussed in this guide, merchants cannot make an ID a condition of acceptance. Therefore, merchants cannot as part of their regular card acceptance procedures refuse to complete a purchase transaction because a cardholder refuses to provide ID. It is important that merchants understand that the requesting of a cardholder ID does not change the merchant’s liability for chargebacks. However, it can slow down a sale and annoy the customer. In some cases, it may even deter the use of the Visa card and result in the loss of a potential sale. Visa believes merchants should not ask for ID as part of their regular card acceptance procedures. Laws in several countries also make it illegal for merchants to write a cardholder’s personal information, such as an address or phone number, on a sales receipt.

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.

---

**Cash Disbursements/Cash Advances**

Generally, merchants are prohibited from making cash disbursements/cash advances. Under special circumstances, certain merchants may dispense 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.
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 high value or 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 value 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 a Code 10 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 point-of-sale 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.

<table>
<thead>
<tr>
<th>At the Counter</th>
<th>At the Pump (Unattended Terminals)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buying more than US $50 worth of convenience store items</td>
<td>Activating multiple pumps</td>
</tr>
<tr>
<td>Buying large amounts of beer and cigarettes</td>
<td>Buying gas several times a day</td>
</tr>
<tr>
<td>Buying tires and not needing them mounted</td>
<td>Filling multiple cars on the same pump</td>
</tr>
<tr>
<td>Attempting to bribe a cashier</td>
<td>Filling large containers</td>
</tr>
<tr>
<td>Asking for cash back with a credit card</td>
<td>Testing cards</td>
</tr>
<tr>
<td></td>
<td>Loitering at the pumps</td>
</tr>
</tbody>
</table>
Skimming

What Is Skimming?
To circumvent the Card Verification Value (CVV) protection, criminals have migrated to “skimming” counterfeit card data. Through new, easy-to-use technology, criminals are capturing full-track 1 and 2 data contained on the magnetic stripe of a legitimate card, and using it to either encode a counterfeit card or re-encode a lost or stolen card. When an electronic authorization attempt is made with the encoded or re-encoded card, it can result in an issuer approval of a fraudulent transaction.

Skimming Prevention at the Merchant Location

• 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.
  – High levels of fallback transactions
  – Apparent tampering with the in-store point-of-sale devices (scratches, color changes, devices attached to point-of-sale cables, etc.)

• Ensure that card data is protected in accordance with PCI DSS at all times. Transmission of card data to other organizations should be compliant with PCI DSS. All payment devices should be compliant with PCI PA-DSS, as well.

• If you suspect skimming activity is happening at your place of business, call your acquirer, law enforcement, and company security immediately.
Code 10 Calls

Code 10 calls allow merchants to alert card issuers to suspicious activity and take appropriate action when instructed to do so. You should make a Code 10 call to your voice authorization center whenever you are suspicious about a card, 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.

The Code 10 Call Process

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 acquirer 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 call at this time may help stop fraudulent card use at another location, or perhaps during a future transaction at your store.
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 and it can be done safely. 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 of this document).
- 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 pages 20 and 21 of this document).
- 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, prepaid 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.
- Make a readable copy of the front and back of the card, if possible.
- If the recovered card is retained by law enforcement officials, you must give your acquirer a readable copy to be eligible for a reward.
- Cut the card according to acquirer procedures.
- Tell your acquirer that you have recovered a card and ask for further instructions.

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

What is Visa payWave?

Merchants can take advantage of increased speed and convenience—and offer these advantages to cardholders—with Visa payWave, a new payment method that uses the latest technology to send card data wirelessly to a terminal reader. A cardholder simply holds their card in front of the reader.

For many transactions, there is no need to sign a receipt or hand over the card. Visa payWave provides merchants and consumers with a number of benefits.

Merchant Benefits

Cost Savings/Efficiency

- Decreased transaction time.
- Customer initiates the transaction by simply holding the card in front of the reader rather than swiping or handing the card to the clerk.
- Reduction in coin/cash handling.

Customer Loyalty

- Attracts new customers and builds loyalty with added speed and convenience.

Competitive Advantage

- Sets merchants apart from their competitors in categories like fast food restaurants where speed and convenience are compelling benefits.

How It Works

1. Merchant terminal is enabled with contactless technology.

2. Consumer holds card in front of the reader and terminal light indicates card has been read.

3. Transaction is completed like any card payment.
Visa Easy Payment Service Transactions

What is Visa VEPS?

Purchases of US $25 and under represent a significant share of all consumer spending. The Visa Easy Payment Service (VEPS) helps deliver greater efficiency and convenience to both merchants and cardholders.

The VEPS program provides face-to-face merchants with the ability to accept a Visa card issued in any country for purchases without requiring a cardholder signature or PIN and foregoing a receipt unless requested by the cardholder. This program has the potential to increase speed at the point-of-sale, enhance customer satisfaction and deliver operating efficiencies for merchants. It can boost customer throughput and build customer loyalty by helping cardholders use their Visa cards safely, quickly and easily.

What are the VEPS Program Qualification Requirements?

Transactions qualify for the VEPS program if they meet the following criteria:
- Value is less than or equal to the country transaction limit
- Face-to-face environment
- Authorized
- Applies in all Merchant Category Codes (MCCs), except those listed in the table on the next page
- Terminal must read and transmit unaltered magnetic stripe track data, unaltered chip data, or unaltered contactless payment data

Visa Easy Payment Service Transaction Restrictions

The following transactions do not qualify for the VEPS program:
- Fallback transactions
- Account funding transactions
- Cash-back transactions
- Manual cash disbursement transactions
- Quasi-cash transactions
- Prepaid load transactions
- Transactions where Dynamic Currency Conversion is performed

Merchants should discuss VEPS implementation requirements, set-up, and best practices with their acquirer.
Section 2: Card-Present Transactions

How to Process a VEPS Transaction

If eligible, you run the transaction as you normally would and eliminate the steps of PIN entry or checking and collecting the cardholder’s signature. In addition, you only need to provide a transaction receipt if the cardholder requests one.

<table>
<thead>
<tr>
<th>Table: MCCs Excluded from Visa Easy Payment Service Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>4829</td>
</tr>
<tr>
<td>5542</td>
</tr>
<tr>
<td>5960</td>
</tr>
<tr>
<td>5962</td>
</tr>
<tr>
<td>5964</td>
</tr>
<tr>
<td>5965</td>
</tr>
<tr>
<td>5966</td>
</tr>
<tr>
<td>5967</td>
</tr>
<tr>
<td>5968</td>
</tr>
<tr>
<td>5969</td>
</tr>
<tr>
<td>6010</td>
</tr>
<tr>
<td>6011</td>
</tr>
<tr>
<td>7995</td>
</tr>
<tr>
<td>9405</td>
</tr>
<tr>
<td>9700</td>
</tr>
<tr>
<td>9701</td>
</tr>
<tr>
<td>9702</td>
</tr>
<tr>
<td>9751</td>
</tr>
<tr>
<td>9752</td>
</tr>
<tr>
<td>9950</td>
</tr>
</tbody>
</table>
Electron Cards

The Visa Electron card* is issued in certain countries around the world. 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 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, or they may be restricted from any or all these functions.
- Electronic authorization is required for all Electron card transactions. This means you must be able to perform the authorization by swiping the stripe through a point-of-sale terminal, inserting the chip card into the chip-reading device, or waving the card in front of a Visa payWave 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.**

* Visa Electron Card is only available in certain countries, but is accepted worldwide.
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 may either not have a watermark, or it may 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 may 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 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.
Section 3  Card-Absent Transactions

What’s Covered

- General Card-Absent Transaction Procedures
- 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 merchant channels 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 help prevent fraud and chargebacks.
General Card-Absent Transaction Procedures

Card-Absent Transaction Processing Actions

Mail order/telephone order (MO/TO) and Internet merchants must verify—to the greatest extent possible—the cardholder’s identity and the validity of the transaction.

- Always ensure that, at a minimum, you collect the following details from your customer:
  - The card account number
  - The name as it appears on the card
  - The card expiration date as it appears on the card
  - The cardholder’s statement address
- Also check whether the card has a card start date and record this detail.
- If possible, take note of a contact phone number (preferably not a cell phone number) and the name of the financial institution that issued the card.
- If you are taking an order over the telephone:
  - Record the time and date of your conversation.
  - Make a note of the details of the conversation.
  In the event of a query, these details can then be verified with the cardholder.
- If you are taking an order through the mail or via a fax:
  - Obtain a signature on the order form.
  - Always retain a copy of the written order.
  - Get proof of delivery.

Your acquirer may ask that you record some additional information. You should find out what your acquirer requirements are and include them in your transaction processing policies and procedures.

- If available, use fraud prevention tools such as Card Verification Value 2 (CVV2)*, Address Verification Service (AVS)**, and Verified by Visa.
- Perform internal screening (e.g., velocity checks, negative database, etc.) or use third party tools to screen for questionable transaction data or other potential warning signs indicating “out of pattern” orders. Route transactions with higher risk characteristics for fraud review.

* In certain markets, CVV2 is required to be present for all card-absent transactions.
** AVS is only available in the U.S. and Canada.
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 the card at the time of an order. (See Visa Card Features and Security Elements in Section 2: Card-Present Transaction of this manual.)

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.
- If the customer provides a CVV2, submit this information with other transaction data (i.e., card expiration date and account number) for electronic authorization.

* In certain markets, CVV2 is required to be present for all card-absent transactions.
You should also include one of the following CVV2* presence indicators, even if you are not including a CVV2 in your authorization request:

<table>
<thead>
<tr>
<th>If:</th>
<th>Send this Indicator to the Card Issuer:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have chosen not to submit CVV2</td>
<td>0</td>
</tr>
<tr>
<td>You included CVV2 in the authorization request</td>
<td>1</td>
</tr>
<tr>
<td>Cardholder has stated CVV2 is illegible</td>
<td>2</td>
</tr>
<tr>
<td>Cardholder has stated CVV2 is not on the card</td>
<td>9</td>
</tr>
</tbody>
</table>

After receiving a positive authorization response, evaluate the CVV2 result code and take appropriate action based on all transaction characteristics.

<table>
<thead>
<tr>
<th>Result:</th>
<th>Action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>M – Match</td>
<td>Complete the transaction (taking into account all transaction characteristics and any questionable data).</td>
</tr>
<tr>
<td>N – No Match**</td>
<td>View the “No-Match” as a sign of potential fraud and take it into account along with the authorization response and any other questionable data. Potentially hold the order for further verification.</td>
</tr>
<tr>
<td>P – Not Processed</td>
<td>View the “Not Processed” as a systemic technical problem or the request did not contain all the information needed to verify the CVV2 code. Resubmit the authorization request.</td>
</tr>
<tr>
<td>S – CVV2 should be on the card</td>
<td>Consider following up with your customer to verify that he or she checked the correct card location for CVV2. All valid cards are required to have CVV2 printed either in the signature panel or in a white box to the right of the signature panel.</td>
</tr>
<tr>
<td>U – Card issuer does not participate in the CVV2 service</td>
<td>Evaluate all available information and decide whether to proceed with the transaction or investigate further.</td>
</tr>
</tbody>
</table>

Merchants should check with their acquirer regarding CVV2 result code evaluation decisions and appropriate actions.

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.

* In certain markets, CVV2 is required to be present for all card-absent transactions.
** In some markets, if the transaction is approved, but the CVV2 response is a no match, the merchant is protected against fraud chargebacks.
The Address Verification Service (AVS)* allows card-absent merchants to check a Visa cardholder’s billing address with the card issuer. An AVS request includes the billing address (street address and/or zip or postal code). It can be transmitted in one of two ways:

1. As part of an authorization request, or
2. By itself. AVS checks the address information and provides a result code to the merchant that indicates whether the address given by the cardholder matches the address on file with the card issuer.

AVS can only be used to confirm addresses in the U.S., and Canada. In other countries, card issuer participation is optional.

AVS Processing Options

AVS Processed as Part of an Authorization Request

The AVS request can be processed either on a real-time basis or in a batch mode using an electronic terminal or personal computer. Real-time requests are typically used for transaction situations where the customer must wait online for a response. The batch mode is geared more toward lower-cost processing for which no immediate response is required as is usually the case with mail orders.

AVS Processed As Part of Account Verification Request

A merchant may also send an AVS request without an accompanying authorization request by using the Zero Amount Account Number Verification Service**, which is available in all regions. For example:

- The merchant wants to verify the customer’s billing address before requesting an authorization, or
- The merchant sends an authorization request with AVS data and receives an authorization approval, but also receives an AVS “try again later” response.

---

* AVS is only available in the U.S. and Canada.
** For more information regarding the Zero Amount Account Number Verification Service, contact your acquirer.
How to Use AVS

Whether AVS* is processed as part of an authorization request, or without it using account verification, the process is as follows:

- When a customer contacts you to place an order,
  - Confirm the usual order information.
  - Ask the customer for the billing address (street address and/or zip or postal code) for the card being used (i.e., the billing address is where the customer’s monthly Visa statement is sent for the card being used).
  - Enter the billing address and the transaction information into the authorization request system and process both requests at the same time.

- The card issuer will make an authorization decision separately from the AVS request and compare the cardholder billing address sent with the billing address for that account. The card issuer will then return both the authorization response and a single character alphabetic code result that indicates whether the address given by the cardholder matches the address on file with the card issuer.

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.

---

* AVS is only available in the U.S. and Canada.
** In certain markets, CVV2 is required to be present for all card-absent transactions.
AVS Result Codes

One of the following AVS* result codes will be returned to the merchant indicating the card issuer’s response to the AVS request. A merchant’s acquirer may modify these single character alpha AVS codes to make them more self-explanatory—for example, a “Y” response may be shown by the acquirer as an “exact match” or as a “full match,” while an “N” response may be shown as a “no match.”

<table>
<thead>
<tr>
<th>Code</th>
<th>Definition</th>
<th>Code Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Domestic</td>
</tr>
<tr>
<td>A</td>
<td>Street addresses match. The street addresses match but the postal or ZIP codes do not, or the request does not include the postal or ZIP code.</td>
<td>✔️</td>
</tr>
<tr>
<td>B</td>
<td>Street addresses match. Postal or ZIP code not verified due to incompatible formats. (Acquirer sent both street address and postal or ZIP code.)</td>
<td>✔️</td>
</tr>
<tr>
<td>C</td>
<td>Street address and postal code or ZIP code not verified due to incompatible formats. (Acquirer sent both street address and postal or ZIP code.)</td>
<td>✔️</td>
</tr>
<tr>
<td>D</td>
<td>Street addresses and postal or ZIP codes match.</td>
<td>✔️</td>
</tr>
<tr>
<td>F</td>
<td>Street addresses and postal codes match. (Applies to U.K.-domestic transactions only.)</td>
<td>✔️</td>
</tr>
<tr>
<td>G</td>
<td>Address information not verified for international transaction. Card issuer is not an AVS participant, or AVS data was present in the request but card issuer did not return an AVS result, or Visa performed address verification on behalf of the card issuer and there was no address.</td>
<td>✔️</td>
</tr>
<tr>
<td>I</td>
<td>Address information not verified.</td>
<td>✔️</td>
</tr>
<tr>
<td>M</td>
<td>Street address and postal and ZIP codes match.</td>
<td>✔️</td>
</tr>
<tr>
<td>N</td>
<td>No match. Acquirer sent postal or ZIP code only, or street address only, or both postal or ZIP code and street address.</td>
<td>✔️</td>
</tr>
<tr>
<td>P</td>
<td>Postal or ZIP codes match. Acquirer sent both postal or ZIP code and street address, but street address not verified due to incompatible formats.</td>
<td>✔️</td>
</tr>
<tr>
<td>R</td>
<td>Retry. System unavailable or timed out. Card issuer ordinarily performs address verification but was unavailable. Visa uses code R when card issuers are unavailable.</td>
<td>✔️</td>
</tr>
<tr>
<td>U</td>
<td>Address information is unavailable for that account number, or the card issuer does not support.</td>
<td>✔️</td>
</tr>
<tr>
<td>Y</td>
<td>Street address and postal and ZIP code match.</td>
<td>✔️</td>
</tr>
<tr>
<td>Z</td>
<td>Postal or ZIP codes match, street addresses do not match or street address not included in request.</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Please contact your acquiring bank for further questions on AVS result codes.

* AVS is only available in the U.S. and Canada.
** In certain markets, CVV2 is required to be present for all card-absent transactions.
While Visa does not recommend any particular approach, the following general guidelines are drawn from card-absent industry practices and may be helpful. Merchants should establish their own policy regarding the handling of transactions based on AVS* result codes.

<table>
<thead>
<tr>
<th>U.S. Code</th>
<th>Int’l Code</th>
<th>Definition</th>
<th>Explanation</th>
<th>Action(s) to Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>D F M</td>
<td><strong>Exact Match</strong></td>
<td>Both street address and ZIP or Postal Code match.</td>
<td>Generally speaking, you will want to proceed with transactions for which you have received an authorization approval and an “exact match.”</td>
</tr>
<tr>
<td>A</td>
<td>B</td>
<td><strong>Partial Match</strong></td>
<td>Street address matches, but ZIP or Postal Code does not.</td>
<td>You may want to follow up before shipping merchandise. The card issuer might have the wrong ZIP or Postal Code in its file; merchant staff may have entered the ZIP or Postal Code incorrectly; or this response may indicate a potentially fraudulent situation.</td>
</tr>
<tr>
<td>Z</td>
<td>P</td>
<td><strong>Partial Match</strong></td>
<td>ZIP Code matches, but street address does not.</td>
<td>Unless you sent only a ZIP or Postal Code AVS request and it matched, you may want to follow up before shipping merchandise. The card issuer may have the wrong address in its file or have the same address information in a different format; the cardholder may have recently moved; merchant staff may have entered the address incorrectly; or this response may indicate a potentially fraudulent situation.</td>
</tr>
<tr>
<td>N</td>
<td>N</td>
<td><strong>No Match</strong></td>
<td>Street address and ZIP or Postal Code do not match.</td>
<td>You may want to follow up with the cardholder before shipping merchandise. The cardholder may have moved recently and not yet notified the card issuer; the cardholder may have given you the shipping address instead of the billing address; or the person may be attempting to execute a fraudulent transaction. “No match” responses generally result in further merchant investigation.</td>
</tr>
</tbody>
</table>

AVS result codes and explanation provided here are meant to give you enough information to make your own determination of what works best for you. How one merchant treats these codes may be different than the way another merchant treats the same codes.

On ZIP or Postal Code only requests and P.O. Box addresses, card issuers may respond either with a “Y” (Exact Match) or a “Z” (Partial Match — ZIP Code/Postal Code Matches).

* AVS is only available in the U.S. and Canada.
Section 3: Card-Absent Transactions

International Addresses

AVS* can only be used to confirm addresses in the U.S. and Canada. If you submit an address outside the U.S. and Canada 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 otherwise 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 acquirer. To request an address verification, call the MDAS toll-free number. 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.

<table>
<thead>
<tr>
<th>MDAS Response</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exact Match</td>
<td>Street address and zip code match.</td>
</tr>
<tr>
<td>Partial Match</td>
<td>Street address matches, but not zip code.</td>
</tr>
<tr>
<td>Partial Match</td>
<td>Zip code matches, but not street address.</td>
</tr>
<tr>
<td>No Match</td>
<td>Neither street address nor zip code matches.</td>
</tr>
<tr>
<td>Retry Later</td>
<td>Card issuer system is not available at present.</td>
</tr>
<tr>
<td>Global</td>
<td>International address; cannot be verified.</td>
</tr>
</tbody>
</table>

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

---

* AVS is only available in the U.S. and Canada.
** MDAS is only available in the U.S.
Section 3: Card-Absent Transactions

Merchant Website Requirements

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

- **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 17.)

- **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 acquirer to ensure your disclosure is made in accordance with the Visa International Operating Regulations and local law.

- **Export restrictions (if known).**

Best Practices for the Web

Suggested best practices for merchant website information 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.

- **A statement on website regarding security controls used to protect customers.**

- **A statement encouraging cardholders to retain a copy of the transaction receipt.**

Your acquirer may require that your merchant website include certain of the above elements.
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 provides cardholder authentication for online transactions. Based on the 3-D Secure protocol, the Verified by Visa service verifies the authenticity of cardholders to participating merchants. It allows cardholders to choose a password through their card issuer, and use it to authenticate themselves while making a purchase. This helps ensure that their card number cannot be fraudulently used at an Internet merchant website.

Cardholders sign up for the Verified by Visa service through their issuing financial institution and choose their own personal password to authenticate themselves online.

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. Merchants who opt to implement Verified by Visa should use PCI compliant vendors and payment solutions.

Verified by Visa Activation

To use Verified by Visa, cardholders must first activate their existing card(s) for the Verified by Visa service. There are a number of ways they may do this:

- Card issuers typically provide an online activation site.
- Visa, card issuers, and participating merchants may display “Activation Anytime”* banners or buttons that enable cardholders to activate their Visa card.
- Cardholders may also activate during the shopping experience, where available.

If the cardholder chooses to activate during shopping, he or she provides information to their Visa card issuer for identification purposes. The cardholder then creates a password. On future purchases at participating online stores, the cardholder's Verified by Visa password will be required during checkout, reducing the potential for fraudulent use of the card.

Verified by Visa Shopping

Once Verified by Visa is activated, a consumer’s card is automatically recognized when used for purchases at participating online stores. The consumer is asked for their password; the password is verified; and the transaction is completed. If the password is not verified cardholder is not confirmed, an error message appears and the transaction should not be completed.

* Activation Anytime is only available in the U.S.
If you are a Verified by Visa merchant:

- Add the Verified by Visa logo on your home, security information, and checkout pages to promote reliable and secure online shopping. Use one of these two approaches:
  - **Activation Anytime**—This is the preferred approach that guides your customers directly to an activation page where they can activate their Visa cards for the Verified by Visa service without leaving your site.
  - **Learn More**—This approach directs your customers to a service description page (hosted by your site) where they can read more about Verified by Visa and activate their cards for the Verified by Visa service. Be sure to provide clear instructions on how Verified by Visa works. Your merchant toolkit includes a “Learn More” page that details the Verified by Visa program. The merchant toolkit is available on [www.visa.com](http://www.visa.com).

- Add a pre-authentication message on the checkout page to inform customers that they may be asked to activate their Visa card for Verified by Visa.

- **Complete the Verified by Visa authentication process.** Provide the authentication data in the VisaNet authorization request as appropriate.

- **If Verified by Visa authentication fails, request payment by alternate means.**
  - Quickly display a message or page to communicate to the cardholder that the purchase will not be completed with the card that failed.
  - Offer an immediate opportunity for the cardholder to enter a new payment card number and try again, or
  - Present a button that, when clicked, opens a new page that allows the cardholder to reinitiate the purchase.

- **Do not submit an authorization request for Verified by Visa transactions that fail authentication.**

---

*Activation Anytime is only available in the U.S.*
Verify by Visa Merchant Chargeback Protection

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

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

Fraud Screening

Today, a wide variety of fraud-screening services and practices is 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 Risk Management Solutions.

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 country.

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.

* A Verified by Visa merchant identified by the Merchant Fraud Performance (MFP) program may be subject to chargeback Reason Code 93: Merchant Fraud Performance Program.
** AVS is only available in the U.S. and Canada.
*** In certain markets, CVV2 is required to be present for all card-absent transactions.
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 or low-value transactions—those with potential losses that are less than the cost of scoring—and eliminating them from the scoring process.

CyberSource Risk Management Solutions*

CyberSource Risk Management Solutions provides fraud detection for organizations of all sizes. Decision Manager and Managed Risk Services** are ideal for mid-to-large companies; Authorize.Net Advanced Fraud Detection Suite™ (AFDS)*** is geared towards small businesses.

- **Decision Manager and Managed Risk Services** enable mid-size to large companies to detect fraud more accurately, review more efficiently, and improve control over fraud management practices, across all card brands and payment methods. Decision Manager utilizes the widest breadth of data in the market (from the specific merchant, from CyberSource’s multi-merchant database, and all transactional data from Visa), and correlates the data to identify fraudulent activity.

- **CyberSource Decision Manager** comes with over 200 detectors, a powerful statistical model built with Visa, a case management system, and detailed reporting. Merchants can supplement Decision Manager with Managed Risk Services, whereby CyberSource fraud analysts provide consultation and recommendations on improving fraud management processes.

- **Authorize.Net Advanced Fraud Detection Suite (AFDS)** is a set of customizable, rules-based filters and tools that help small businesses identify, manage, and prevent suspicious and potentially costly fraudulent transactions. Multiple filters and tools work together to evaluate transactions for indicators of fraud. Their combined logic provides a powerful and highly effective defense against fraudulent transactions. Filters include transaction velocity, IP checks, address mismatches, and more. AFDS is also integrated with the Address Verification Service (AVS) and Card Verification Value 2 (CVV2). Authorize.Net AFDS is a value-added service of the Authorize.Net Payment Gateway.

* CyberSource is a wholly-owned subsidiary of Visa.
** CyberSource Decision Manager and Managed Risk Services are available globally.
*** Authorize.Net Advanced Fraud Detection Suite is available in the United States.
Merchants that implement CyberSource Risk Management Solutions experience several important benefits.

- Increased sales conversion: Generate more order approvals as a result of improved risk-assessment accuracy.
- Fewer chargebacks: Lower direct and indirect costs associated with the management of fraudulent transactions.

**Direct costs**
- Loss of product
- Order shipping and handling costs

**Indirect costs (chargeback-related)**
- Bank fees
- Customer service staff time
- Cash management and discount rates

- Improved customer satisfaction: Increase valid order processing due to the automated fraud screening, allowing your customers to receive goods and services in a timely manner, and reducing customer insult from incorrectly rejecting valid orders.

To learn more about the CyberSource Risk Management Solutions (for mid-size to large companies) visit www.cybersource.com or (for small business) www.authorize.net.

For a copy of the CyberSource Online Fraud Report, white papers regarding online fraud or payment security, visit www.cybersource.com.

For information on Authorize.Net Advance Fraud Detection Suite, visit www.authorize.net.
Section 3: Card-Absent Transactions

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:

- **Rush orders:** Urgent requests for quick or overnight delivery—the customer who “needs it yesterday”—should be red flagged 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.

- **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.

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.

Experience suggests that Internet orders with certain characteristics can be tip-offs to possible fraud. Suspicous 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.

Guidelines for Internet Merchants

- **Rush orders:** Urgent requests for quick or overnight delivery—"needs it yesterday"—should be red flagged 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.

- **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.
Characteristics to watch out for include:

- **First-time shopper**: Criminals are always looking for new merchants to steal from.
- **Larger-than-normal orders**: Because stolen cards or account numbers have a limited life span, criminals need to maximize the size of their purchase.
- **Orders that include several varieties of the same item**: Having multiples of the same item increases criminal’s profits.
- **Orders made up of “big-ticket” items**: These items have maximum resale value and therefore maximum profit potential.
- **“Rush” or “overnight” shipping**: Criminals want their fraudulently obtained items as soon as possible for the quickest possible resale and aren’t concerned about extra delivery charges.
- **Shipping outside of the merchant’s country**: There are times when fraudulent transactions are shipped to fraudulent criminals outside of the home country.

An important Visa fraud prevention tool designed to help combat this type of risk is the **Address Verification Service (AVS)**. AVS enables a card-absent merchant to verify a credit or debit card billing address of the customer who is paying with a Visa card. The merchant includes an AVS request with the transaction authorization and receives a result code (separate from the authorization response code) that indicates whether the address given by the cardholder matches the address in the issuer’s file. A partial or no-match response may indicate fraud risk.

- **Orders from Internet addresses that make use of free e-mail services**: These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

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 with similar account numbers**: May indicate the account numbers used have been generated using software available on the Internet.
- **Shipping to a single address, but transactions placed on multiple cards**: Could involve an account number generated using special software, or even a batch of stolen cards.
- **Multiple transactions on one card over a very short period of time**: Could be an attempt to “run a card” until the account is closed.
- **Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses**: Could represent organized activity, rather than one individual at work.
- **For online transactions, multiple cards used from a single IP (Internet Protocol) address**: More than one or two cards could indicate a fraud scheme.

*AVS is only available in the U.S. and Canada.*
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 (see *Code 10 Calls* in Section 1: Getting Down to Basics).

- **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.

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 to find a cardholder’s telephone number.** Do not use the telephone number given for a suspect transaction.

- **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.
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 charges.
- The period of time the cardholder has agreed to for the charges.

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.

Merchants should determine whether there are requirements under local law for cardholder authorization of recurring transactions, such as a signature requirement.

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, acquirers, and card issuers to exchange electronic updates of cardholder account information.
- Keep the cardholder’s expiration date on file and include it in all authorization requests.

* AVS is only available in the U.S. and Canada.
** In certain markets, CVV2 is required to be present for all card-absent transactions.
• **Use AVS.**

• **Ensure that all recurring transactions are clearly identified as such.** This identification is usually handled automatically by a merchant’s transaction-processing system; however, you should check with your acquirer 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 ten 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. Local law may impose specific requirements for this notification.

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

How the Visa Account Updater (VAU) Service Works

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

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

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

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

• **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.

---

*In certain markets, CVV2 is required to be present for all card-absent 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 in compliance with the requirement of local laws 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.**
With recent media reports of hacker incidents, stolen payment card, PINs, 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.

The Payment Card Industry Data Security Standard (PCI DSS) is intended to help protect Visa cardholder data—wherever it resides—ensuring that merchants and their service providers maintain a high information security standard. It offers a baseline approach to safeguarding sensitive data for all card brands. PCI DSS compliance is required of all entities that store, process, or transmit Visa cardholder account and transaction data, although PCI DSS compliance assessment requirements vary depending on the merchants card transaction volume.

The 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 a high level of PIN security.
What is the PCI DSS?

The PCI DSS is a comprehensive set of international security requirements to help protect cardholder data. The PCI DSS was developed by Visa and the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS consists of twelve basic requirements. These requirements are the foundation of Visa’s data security compliance program known as the Account Information Security (AIS) Program. This program was formerly known as the Cardholder Information Security Program (CISP) in the U.S.

All Visa acquirers and card issuers must comply, and must also ensure the compliance of their merchants and service providers who store, process, or transmit Visa account numbers. This program applies to all payment channels including card-present, mail/telephone order, and e-commerce.

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

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

All Visa members, merchants and service providers must adhere to the PCI DSS twelve basic requirements, which are supported by more detailed sub-requirements.

<table>
<thead>
<tr>
<th>PCI Data Security Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
</tr>
</tbody>
</table>

The PCI DSS can be found at www.pcissc.org.
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, acquiring or merchant activity) must comply with the PCI DSS.

By complying with PCI DSS requirements, merchants not only meet their obligations to the Visa payment system, but also:

**Build Consumer Trust in the Security of Sensitive Information**

Customers seek out merchants that they feel are “safe.” Confident consumers are loyal customers. They come back again and again, as well as share their experience with others.

**Minimize Direct Losses and Associated Operating Expenses**

Appropriate data security helps protect cardholders, limit risk exposure, and minimize the losses and operational expense that stem from compromised cardholder information.

**Maintain Positive Image**

Information security is on everyone’s mind...including the media's. Data loss or compromise not only hurts customers, it can seriously damage a business’s reputation.
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 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 POS PIN-Entry Devices (PEDs).

The program is designed to protect members, merchants, and service providers. It is designed to help ensure the safe management, processing and transmission of cardholder PINs at ATM and point-of-sale PEDs. As a result, members, merchants, and service providers can help 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 the PCI PIN Security Requirements, visit www.visa.com/cisp.
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/cisp, 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/cisp, as needed.

• **Use Compliant Equipment.** Purchase only terminals that have been PCI approved. Work with your acquirer or Encryption and Support Organization (ESO) to create a plan that ensures all deployed attended point-of-sale PEDs are Visa-approved and are using Triple Data Encryption Standards (TDES). For more information on Visa’s PED testing and TDES usage requirements, visit www.visa.com/cisp. 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 point-of-sale 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 acquirer must register the ESO with Visa. For more information, refer to the Visa Cryptographic Key Injection Facility Requirements Manual at www.visa.com/pinsecurity.
• **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 ensure they are in full compliance with Visa’s PED-testing and TDES requirements. Failure to comply could result in a high degree of risk exposure. For more information on Visa’s TDES Interlink Compliance Policy, visit [www.visa.com/cisp](http://www.visa.com/cisp).
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 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 on site as quickly as possible 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.** 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). Visa highly recommends compromised system(s) not be used to avoid losing critical volatile data.
   - Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
   - Preserve evidence and logs (i.e., original evidence, security events, web, database, firewall, etc.)
   - Document 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:
   - Your internal incident response team and information security group.
   - If you are a merchant, contact your acquirer.
   - If you do not know the name and/or contact information for your acquirer, notify Visa Incident Response Manager immediately:
     - U.S. – (650) 432-2978 or usfraudcontrol@Visa.com
     - Canada – (416) 860-3090 or CanadaInvestigations@Visa.com
     - Latin America & Caribbean – (305) 328-1713 or lacrmac@Visa.com
     - Asia Pacific – (65) 96307672 or APInvestigations@Visa.com
     - CEMEA – +44 (0) 207-225-8600 or CEMEAFraudControl@Visa.com
   
   3. Notify the appropriate law enforcement agency. Contact the Visa Incident Response Manager above for assistance in contacting local law enforcement agency.
   
   4. Consult with your legal department to determine if notification laws are applicable.
   
   5. Provide all compromised Visa, Interlink, and Plus accounts to your acquirer or to Visa within ten (10) business days. All potentially compromised accounts must be provided and transmitted as instructed by the Visa acquiring bank and Visa. Visa will distribute the compromised Visa account numbers to card issuers.
   
   6. Within three (3) business days of the reported compromise, provide an Incident Report to the acquirer or to Visa.
   
   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.
Appendix 1: Training Your Staff

Training is Good Business

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

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

- Sales staff and customer service associates benefit because they are given the skills and knowledge they need to do their jobs accurately and confidently.

- You benefit because:
  - Customer service is enhanced, leading to increased sales.
  - You may have fewer fraudulent transactions, which reduces related losses.
  - You may have fewer transaction receipt copy requests and chargebacks, which reduces related expenses.

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

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

Chargeback Management Guidelines for Visa Merchants

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

For a copy of this document, contact your acquirer.
Appendix 1: Training Your Staff
Appendix 2: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account number</td>
<td>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.</td>
</tr>
<tr>
<td>Acquirer</td>
<td>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.</td>
</tr>
<tr>
<td>Address Verification Service (AVS)</td>
<td>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. AVS helps merchants minimize the risk of accepting fraudulent transactions in a card-absent environment by indicating the result of the address comparison.</td>
</tr>
<tr>
<td>ATM</td>
<td>An unattended magnetic-stripe or chip-reading terminal that has electronic capability, accepts PINs, and disburses currency or travelers cheques.</td>
</tr>
<tr>
<td>Authorization</td>
<td>The process by which a card issuer approves or declines a Visa card purchase. Authorization typically occurs automatically when you swipe the magnetic stripe of a payment card through a card reader or dip a chip card in a chip-reading device. See also, Voice Authorization Center.</td>
</tr>
<tr>
<td>“Call” or “Call Center” response</td>
<td>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.</td>
</tr>
<tr>
<td>Card acceptance procedures</td>
<td>The procedures a merchant or merchant employee must follow at the point-of-sale to ensure that a card and cardholder are valid.</td>
</tr>
<tr>
<td>Card expiration date (Expiry)</td>
<td>See “Good Thru” date.</td>
</tr>
<tr>
<td>Cardholder</td>
<td>The person to whom a Visa card is issued.</td>
</tr>
<tr>
<td>Card issuer</td>
<td>A financial institution that issues Visa cards.</td>
</tr>
</tbody>
</table>

* AVS is only available in the U.S. and Canada.
Appendix 2: Glossary

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.

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 environments (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 cards, as specified in the Visa International 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 (CVV)  A unique three-digit “check number” encoded on the magnetic-stripe of all valid cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe-encoded account information and is verified online at the same time a transaction is authorized.

Card Verification Value 2 (CVV2)*  A Visa fraud prevention system used in card-absent transactions to confirm 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.

Chargeback  A transaction that is returned as a financial liability to an acquirer by a card issuer, usually because of a disputed transaction. The acquirer may then return or “charge back” the transaction to the merchant.

Chip  An integrated microchip that is embedded into a plastic credit or debit card.

Chip card  A plastic payment card with an embedded computer chip that communicates information to a chip-reading device during the transaction process.

Chip-initiated transaction  An EMV and VIS-compliant chip card transaction which is processed at a chip-reading device using full-chip data, and limited to Visa and Visa Electron Smart Payment Applications, or EMV and VIS-compliant Plus applications.

Chip-reading device  A point-of-transaction terminal capable of reading, communicating, and processing transaction data from a chip card. The chip card and chip-reading device work together to determine the appropriate cardholder or verification method for transaction (either signature, no signature, or PIN).

* In certain markets, CVV2 is required to be present for all card-absent transactions.
Appendix 2: Glossary

**Code 10 call**
A call made by a sales associate to the merchant’s voice authorization center when the appearance of a card or the actions of a cardholder suggest the possibility of fraud. The term “Code 10” is used so calls can be made without arousing suspicion while the cardholder is present. Specially trained operators then provide assistance to point-of-sale staff on how to handle the transaction.

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

**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.

**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.

**Electron card**
A debit or prepaid card that is issued in countries around the world. The card is currently not issued in the U.S., but is accepted at many U.S. merchant locations. Electron cards have slightly different security features than other Visa cards: the front of the card contains an Electron rather than a dove hologram, and the 16-digit account number is printed, not embossed.

**Electronic Commerce Indicator (ECI)**
A transaction data field used by e-commerce merchants and merchant acquirers to differentiate Internet merchants from other merchant types. Use of the ECI in authorization and settlement messages helps e-commerce merchants meet Visa processing requirements and enables Internet transactions to be distinguished from other transaction types. Visa requires all e-commerce merchants to use the ECI.

**Exception file**
A list of lost, stolen, counterfeit, fraudulent, or otherwise invalid account numbers kept by individual merchants or their third party processors. The exception file should be checked as part of the authorization process, particularly for transactions that are below a merchant’s floor limit.

**Firewall**
A security tool that blocks access from the Internet to files on a merchant’s or third party processor’s server and is used to help ensure the safety of sensitive cardholder data stored on a server.

**Fraud scoring**
A category of predictive fraud detection models or technologies that may vary widely in sophistication and effectiveness. The most efficient scoring models use predictive software techniques to capture relationships and patterns of fraudulent activity, and to differentiate these patterns from legitimate purchasing activity. Scoring models typically assign a numeric value that indicates the likelihood that an individual transaction will be fraudulent.
**“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 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.

**Issuer** A financial institution, or other authorized entity that issues Visa cards to cardholders, and with which each cardholder has an agreement to pay transactions initiated through use of the card.

**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 International Operating Regulations*. The stripe is “read” when a card is swiped through a point-of-sale terminal. On a valid card, the account number on the magnetic stripe matches the account number on the front of the card.

**Magnetic-stripe reader** The component of a point-of-sale device that electronically reads the information on a payment card’s magnetic stripe.

**Mail Order/Telephone Order (MO/TO)** A merchant, market, or sales environment in which mail or telephone sales are the primary or major source of income. See also, *Card-absent*.

**Member** An organization that is a financial institution or other entity authorized by Visa to issue cards and/or sign merchants.

**Merchant agreement** The contract between a merchant and an acquirer under which the merchant participates in the Visa payment system, accepts Visa cards for payment of goods and services, and agrees to abide by certain rules governing the acceptance and processing of Visa transactions. Merchant agreements may stipulate merchant liability with regard to chargebacks and may specify time frames within which merchants are to deposit transactions and respond to requests for information.

**Merchant 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.
### Appendix 2: Glossary

**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 (POS) terminal**
The electronic device used for authorizing and processing Visa card 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/or members. The *Visa International Operating Regulations* refers to three types of processors: authorizing processors, clearing processors, and V.I.P. system users. See also, *VisaNet processor*.

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

**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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Split tender</td>
<td>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.</td>
</tr>
<tr>
<td>Third Party Agents</td>
<td>An entity that provides payment related services, directly or indirectly, to a member and/or stores, processes, or transmits cardholder data. A Third Party Agent must be registered by all Visa members utilizing their services, directly or indirectly.</td>
</tr>
<tr>
<td>Third party processor</td>
<td>A non-member organization that performs transaction authorization and processing, account record keeping, and other day-to-day business and administrative functions for card issuers and acquirers.</td>
</tr>
<tr>
<td>Transaction</td>
<td>The act between a cardholder and a merchant that results in the sale of goods or services.</td>
</tr>
<tr>
<td>Transaction receipt</td>
<td>The paper or electronic record of a Visa card transaction that a merchant submits to an acquirer for processing and payment. In most cases, paper drafts are now generated by a merchant’s point-of-sale terminal. When a merchant fills out a draft manually, it must include an imprint of the front of the card.</td>
</tr>
<tr>
<td>Unsigned card</td>
<td>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.</td>
</tr>
<tr>
<td>Verified by Visa</td>
<td>A Visa Internet payment authentication system that helps validate 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 helps allow the card issuer to verify his or her identity.</td>
</tr>
<tr>
<td>Visa Easy Payment Service (VEPS)</td>
<td>Provides face-to-face merchants with the ability to accept a Visa card issued in any country for purchases of US $25 or under without requiring a cardholder signature or PIN and foregoing a receipt unless requested by the cardholder.</td>
</tr>
<tr>
<td>Visa payWave</td>
<td>A new payment method that sends card data wirelessly to a terminal reader. A cardholder simply holds their card in front of the reader. For many transactions, there is no need to sign a receipt or hand over the card. Visa payWave provides merchants and consumers with a number of benefits.</td>
</tr>
<tr>
<td>VisaNet processor</td>
<td>A processor directly connected to VisaNet. See also, Processor.</td>
</tr>
<tr>
<td>Voice authorization</td>
<td>An authorization obtained by telephoning a voice authorization center.</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Voice authorization center</td>
<td>An operator-staffed center that handles telephone authorization requests from merchants who do not have electronic point-of-sale terminals or whose electronic terminals are temporarily not working, or who have transactions that require special assistance. Voice authorization centers also handle manual authorization requests and Code 10 calls.</td>
</tr>
</tbody>
</table>
Appendix 3: Visa Europe Territory

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

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