Card Acceptance Guidelines
for Visa Merchants

VISA

Table of Contents

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.

Sections 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 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 (MO/TO), and eCommerce transactions. This section also covers Visa fraud prevention tools, such as the Address Verification Service (AVS), Card Verification Value 2 (CVV2)*, and Verified by Visa; requirements for eCommerce websites; and procedures for recurring transactions.

- **Section 4: Payment Card Industry Data Security Standard**—Comprehensive coverage of the Payment Card Industry Data Security Standard (PCI DSS) requirements, with which all merchants and service providers must comply, to help ensure the security of confidential cardholder information.

- **Glossary**—A comprehensive list of terms commonly used in today's payment industry.

- **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.

---

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

Important Note About Country Differences

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 an icon for the country under discussion.

The country icons are as follows:

US   United States

Can   Canada

LAC   Latin America and Caribbean (LAC)

AP   Asia Pacific (AP)

CEMEA   Central Europe, Middle East, and Africa (CEMEA)

Guide Navigation

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

Additional insights related to the topic that is being covered.

A brief explanation of the Visa service or program pertinent to the topic at hand.

Disclaimer

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 Core Rules and Visa Product and Service Rules*. If there are any differences between the *Visa Core Rules and Visa Product and Service Rules* and this guide, the *Visa Core Rules and Visa Product and Service Rules* will prevail in every instance. Your merchant agreement and the *Visa Core Rules and Visa Product and Service Rules* take precedence over this guide or any updates to its information. To access a copy of the *Visa Core Rules and Visa Product and Service Rules*, visit www.visa.com.

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, please contact your acquirer.

SECTION 1

Getting Down to Basics

What's Covered

- Visa Transaction Processing—Who is Involved?
- Visa Transaction Flow for Magnetic-Stripe and Contact/Contactless
- Visa Transaction Flow for SMS-Based Point-of-Sale and ATM
- Visa Rules for General Processing
- Visa Rules for Returns and Exchanges
- Visa Rules for PIN-less Payment Brand Acceptance (U.S. Only)
- Visa U.S. Common Debit AID
- Ensuring Merchant Name and Merchant Category Code (MCC) Accuracy

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, there are several other parties that can be involved in the Visa transaction process. 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.

A Payment Facilitator (PF) can enter into a contract with an acquirer to provide payment services to a sponsored merchant.

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 Contact/Contactless 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.**
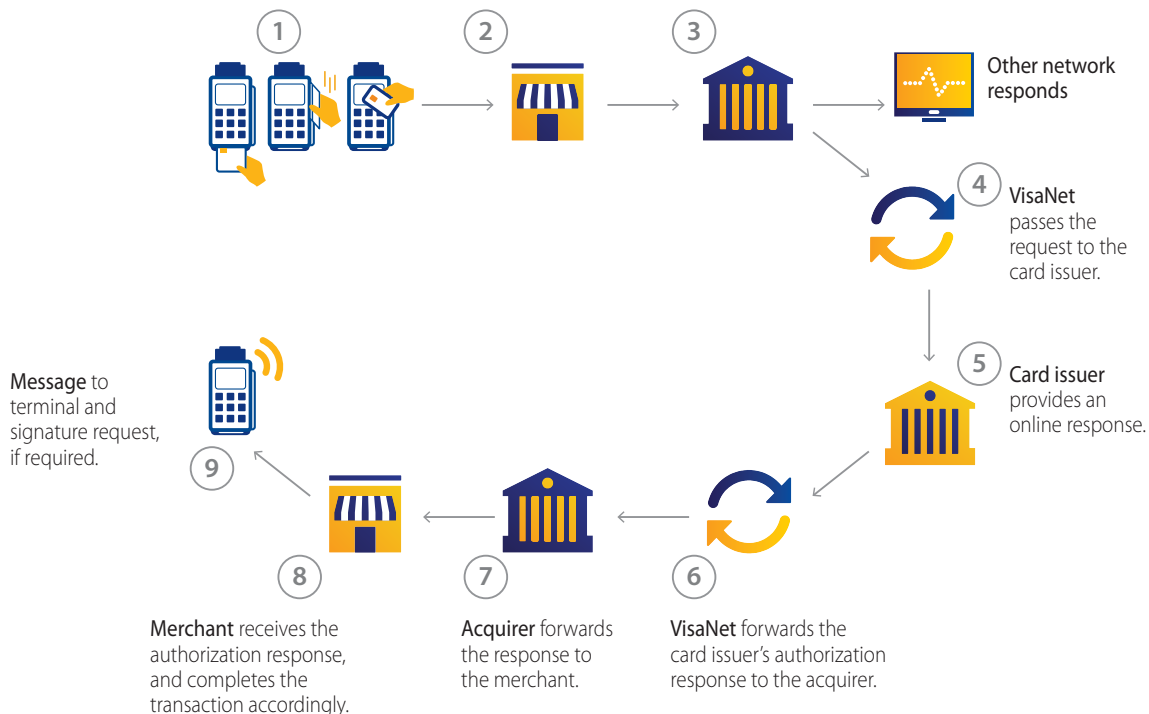
Online Authorization Process for Credit or Debit Transactions

During the **authorization** process, Visa card transactions are approved or declined by the issuer, or by Visa on the issuer's behalf.

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

Merchant enters the transaction amount, and, if necessary, sends an authorization request to the acquirer.*

Acquirer electronically sends the authorization request to VisaNet or determines the network to which the transaction should be routed.

1 2 3

Other network responds

4 VisaNet passes the request to the card issuer.

5 Card issuer provides an online response.

Message to terminal and signature request, if required.

9

8 7 6

Merchant receives the authorization response, and completes the transaction accordingly.

Acquirer forwards the response to the merchant.

VisaNet forwards the card issuer's authorization response to the acquirer.

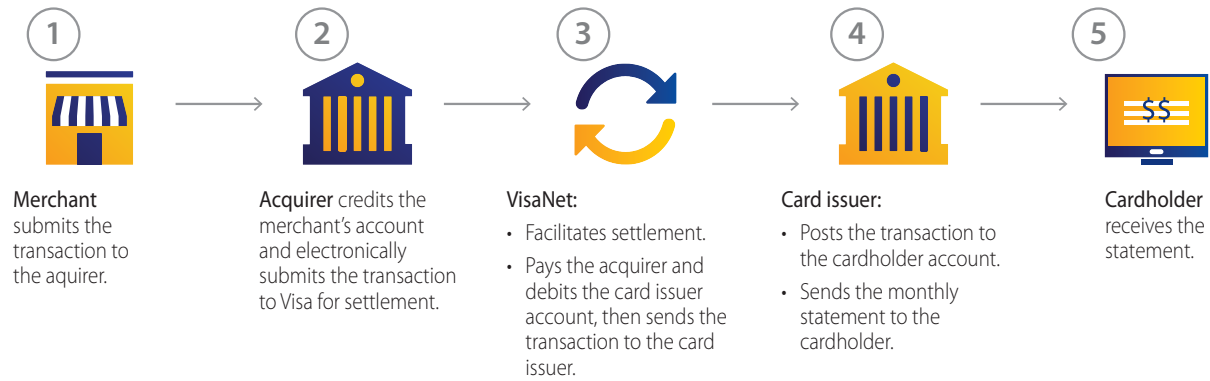**Note: Payment Facilitator (PF) –** In some circumstances, a Payment Facilitator (PF) may transmit the authorization request and response between the merchant and the acquirer. The potential presence of a PF during the transaction process is dependent on acquirer and merchant payment service contractual agreement with the PF.

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

Process of Clearing and Settlement of a Transaction

During the clearing and settlement of a transaction, the transaction information moves from acquirers to card issuers for posting to cardholders' accounts. VisaNet facilitates the payment to the acquirer for a Visa transaction and the debit to the card issuer.

1

Merchant submits the transaction to the aquirer.

2

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

3

VisaNet:
- Facilitates settlement.
- Pays the acquirer and debits the card issuer account, then sends the transaction to the card issuer.

4

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

5

Cardholder receives the statement.

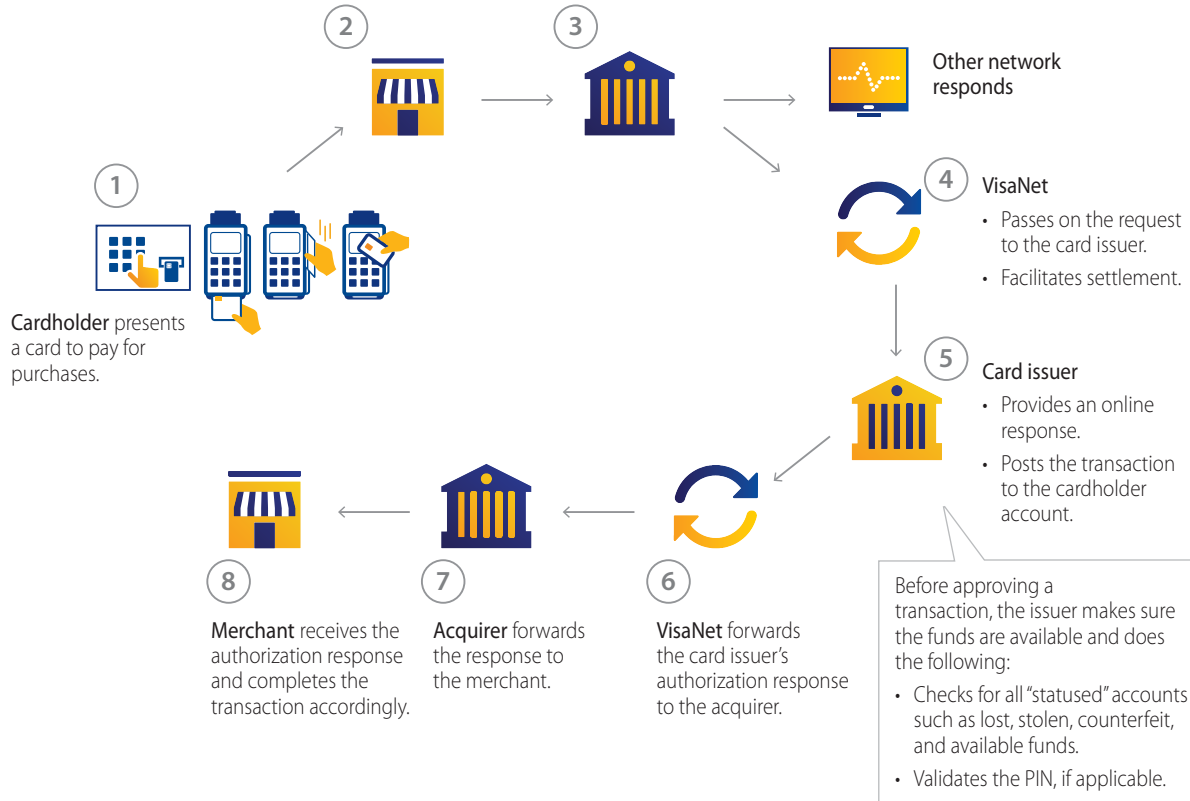# Visa Transaction Flow for SMS-Based Point-of-Sale and ATM

In some cases, POS and ATM transactions are authorized and cleared (posted) at the same time within a single message. This is sometimes referred to as an "online" or "Single-Message System (SMS)" debit transaction. Settlement occurs from single message processing at certain cut-off times during the day. The following diagrams illustrate the basic processing steps for a single message POS (Visa/Interlink) and ATM (Visa/Plus) transaction.

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

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

For **Visa, Interlink or Visa Electron**, the acquirer or back office electronically sends the authorization request to VisaNet.

All other transactions are transmitted to the appropriate network.

2

3

Other network responds

1

Cardholder presents a card to pay for purchases.

4 VisaNet
- Passes on the request to the card issuer.
- Facilitates settlement.

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

8

Merchant receives the authorization response and completes the transaction accordingly.

7

Acquirer forwards the response to the merchant.

6

VisaNet forwards the card issuer's authorization response to the acquirer.

Before approving a transaction, the issuer makes sure the funds are available and does the following:
- Checks for all "statused" accounts such as lost, stolen, counterfeit, and available funds.
- Validates the PIN, if applicable.

Note: Payment Facilitator (PF) – In some circumstances, a Payment Facilitator (PF) may transmit the authorization request and response between the merchant and the acquirer. The potential presence of a PF during the transaction process is dependent on acquirer and merchant payment service contractual agreement with the PF.

Card Acceptance Guidelines for Visa Merchants

Visa Rules for General Processing

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.

Card Acceptance

Accept all types of valid Visa cards. To offer the broadest possible range of payment options to cardholder customers, merchants must accept all categories of Visa debit, credit, and prepaid cards.
Note: Visa debit and credit cards may have different acceptance policies if you are located in the U.S., Australia, New Zealand, or Canada. For specifics on regional differences, refer to the *Visa Core Rules and Visa Product and Service Rules* at www.visa.com.

Surcharges

Surcharges are not permitted, except in the U.S. and AP (Australia and New Zealand).

LAC **US**	In the U.S. region or in a U.S. territory (e.g., Guam in AP and Puerto Rico in LAC), a registered merchant may assess a fixed or variable surcharge on a Visa credit card transaction, subject to certain conditions and applicable laws or regulations. Additional information about U.S. conditions is available at www.visa.com.
AP	In the AP (Australia and New Zealand) region, a merchant may access a fixed or variable surcharge on a Visa transaction, subject to certain conditions and applicable laws or regulations.
	To ensure surcharges are properly assessed, please contact your acquirer.

Minimum Transaction Amount

US	**Ensure minimum transaction amounts, which may be no greater than $10, are imposed on Visa credit card transactions only.** Merchants in the U.S. or a U.S. territory may impose a minimum transaction amount on a Visa credit card. For specifics on regional differences, refer to the *Visa Core Rules and Visa Product and Service Rules* at www.visa.com.

Prohibited Uses

Visa cards must never be used for illegal purposes. Also, merchants must 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).

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.

Convenience Fees

US
CEMEA
AP

For merchants who offer an alternate payment channel (i.e., mail, telephone, or eCommerce) 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.

US
AP

An AP or U.S. merchant that charges a convenience fee must ensure that the fee is:

- Charged for a bona fide convenience in the form of an alternative payment channel (i.e., mail, telephone, eCommerce) outside the merchant's customary payment channels (i.e., not solely for the acceptance of the Visa card).

- Disclosed clearly to the cardholder as a charge for the alternative payment channel convenience.

- Disclosed before the completion of the transaction and the cardholder is given the opportunity to cancel.

- Added only to a transaction completed in a card-absent environment.

- A flat or fixed amount, regardless of the value of the payment due**.

- Applicable to all forms of payment accepted in the payment channel.

- Included as part of the total amount of the transaction.

The Convenience Fee must not be:

- Charged by any third party.

- Added to a recurring transaction.

Further, in the U.S. region or in a U.S. territory, a merchant that assesses a surcharge on a Visa credit card transaction must not charge a convenience fee in addition to the surcharge.

Government and Education Payment Program Service Fee

Properly disclose and process any Government and Education Payment Program Service fees.

In the U.S. region, a government or education merchant may assess a fixed or variable service fee for processing a Visa card transaction if the service fee is:

US

- Clearly disclosed before the completion of the transaction and the cardholder is given the opportunity to cancel.

- Processed as a separate transaction. The government authority or education institution (i.e., merchant) or the third-party service provider will be assigned a unique MVV once the submitted registration form has been approved by Visa. The registered MVV/acquirer BIN combination(s) must be included in all payment clearing transactions (including the service fee transactions) in order to be eligible for the program. The MVV, MCC and acquirer BIN

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

** In AP, an ad valorem amount is allowed where the merchant's pricing is subject to regulatory controls that make a flat fee infeasible.

Card Acceptance Guidelines for Visa Merchants

US in the transactions must match the MVV, MCC and acquirer BIN maintained by Visa. The payment and service fee transactions must be submitted and processed as two separate transactions.

The government and education transaction must include:

- Government authority or education institution (merchant) name in the Merchant Name field (e.g., "U.S. Treasury Tax Payment" for federal tax payments or "CA DMV" for state automobile registration payments; merchant name cannot exceed 25 characters in length)
- Customer support phone number in the Merchant City field
- State of the merchant in the Merchant State field

The service fee transaction must include:

- Merchant or service provider name in the first 3,7, or 12 positions followed by an asterisk (*) in the next position, followed by the words "Service Fee"
- Customer support phone number in the Merchant City field
- State of the service provider in the Merchant State field

To receive the most favorable interchange rate, all debit/credit/commercial transactions must be CPS qualified.

Note: Exempt, card-not-present consumer debit tax payment transactions are still eligible to qualify for the Debit Tax Payment incentive interchange rate provided they are registered for the Government and Education Payment Program. Registered participants are permitted to assess a variable service fee on these transactions with a separate service fee transaction. For more information on how to qualify for the consumer debit tax payment interchange fee program, please refer to the current U.S. Interchange Reimbursement Fee Rate Qualification Guide. All transactions from participating government and education authorities must be submitted according to the Government and Education Payment Program. Participating merchants may access the Debit Acceptance Tables to determine if the transaction was made with a consumer debit card or other card type.

The service fee must be disclosed to the cardholder as a fee assessed by the merchant or the third party.

A merchant participating in the Government and Education Payment Program must not:

- Charge a convenience fee in addition to the service fee.
- Assess a service fee in addition to the U.S. credit card surcharge.

CEMEA **In the CEMEA region (Russia and Egypt only), a merchant may assess a government service fee.** To ensure service fees are properly assessed, 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.

Tips

US In the U.S. for restaurant, taxicab, limousine, bar, tavern, beauty/barber shop, and health/ beauty spa merchant transactions with a Visa credit or debit card, may receive tips from their customers. They must never estimate the tip, but must follow Visa procedures. 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. This practice applies to magnetic-stripe and chip transactions.

In some restaurant environments, if tip is not known when the authorization occurs, the merchant must authorize only the known amount, but may clear for up to 20 percent greater than the authorized amount. If the tip is greater than 20 percent, the merchant may obtain a second authorization.

> 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 hotel, car rental, and cruise line merchants. For car rental, this threshold is the greater of 15 percent or $75.00.

For further information on tips authorization, contact your acquirer.

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. For the most part, 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. There are deadlines by which an acquirer must process the transaction.

Suppressed Account Number and Expiration Date

Ensure that the Visa account number is suppressed in accordance with Visa Rules and local laws and regulations. Effective 1 October 2014, Visa requires the account number be partly suppressed on the receipt; however, rules will vary by region.

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 have been shipped or services received.

Deposits

For transactions where the cardholder pays a deposit, 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 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 deposit 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

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

Cardholder Information

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

> For more information on Visa's data security requirements and programs, see *Section 4: Payment Card Industry Data Security Standard* and the *Qualified Integrators and Resellers Program.*

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 Core Rules and Visa Product and Service Rules***.** 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, transmitting, or has access to 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, POS integrator, 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, as applicable.

In response to merchant breaches caused by payment applications improperly installed by integrators and resellers, Visa recommends that merchants who use POS integrators use certified integrators or resellers from the Payment Card Industry Security Standards Council Qualified Integrators and Resellers (QIR) Program. The QIR program provides payment application developers, integrators and resellers with the training to help merchants and industry participants install and configure validated PA-DSS payment applications in a manner that ensures a merchant's PCI DSS compliance.

Many merchant POS systems are set up with remote access services so that integrators and resellers can provide monitoring and software support. If remote access to the POS system is not configured or maintained in compliance with PCI DSS and PA-DSS (e.g., with default or shared remote access IDs without two-factor authentication or regular password changes), merchants can be infected with malware that puts them at risk for breaches and cardholder data compromises.

The global list of QIRs is located on [www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php.](www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php)

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 Core Rules and Visa Product and Service Rules*.

Any Third Party Agent that is used by a merchant must be validated for PCI DSS compliance, as applicable, and listed on the Visa Global Registry of Service Providers. The global list of PCI DSS Validated Service Providers is located on www.visa.com/splisting.

Sensitive Data Storage and Payment Application Use

Ensure all stored, processed or transmitted sensitive cardholder account or transaction information complies with the PCI DSS and the *Visa Core Rules and Visa Product and Service Rules.* 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.

> For more information on Visa's data security requirements and programs, see *Section 4: Payment Card Industry Data Security Standard.*

Visa Rules for Returns, Exchanges and Cancellations

As a merchant, you are responsible for establishing your merchandise return and refund or cancellation 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. For face-to-face or eCommerce environment, the cardholder must receive the disclosure at the time of purchase. For guaranteed reservations made by telephone, the merchant may send the disclosure after by mail, email or text message.

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

Disclosure for Card-Present Merchants

For card-present transactions, Visa will accept that proper disclosure has occurred before a transaction is completed if the following (or similar) disclosure statements are legibly printed on the face of the transaction receipt near the cardholder signature area or in an area easily seen by the cardholder. If the disclosure is on the back of the transaction receipt or in a separate contract, it must be accompanied by a space for the cardholder's signature or initials.

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

Disclosure for Card-Absent Merchants

Phone Order

For proper disclosure, your refund and credit policies may be mailed, emailed, or texted to the cardholder. As a reminder, the merchant must prove the cardholder received or acknowledged the policy in order for the disclosure to be proper.

Internet or Application

Your website must communicate its refund policy to the cardholder in either of the following locations:

· In the sequence of pages before final checkout, with a "click to accept" or other acknowledgement button, checkbox, or location for an electronic signature, **or**

· On the checkout screen, near the "submit or click to accept button

The disclosure must not be solely on a link to a separate web page.

Visa U.S. Common Debit AID

This section outlines Visa's approach for supporting the Visa U.S. Common Debit AID at POS and ATMs. The Visa U.S. Common Debit AID is intended for U.S. domestic use only including all 50 states, the District of Columbia, and the territories that comprise the United States of America.

Note: The information in this section is based, in part, on the EMF U.S. Debit Technical Solution white paper developed by the EMV Migration Forum (EMF) Debit Technical Working Group.

Note: While each payment scheme has its own U.S. Common Debit AID, all references to this term in this section refer to the Visa U.S. Common Debit AID ('A0 00 00 00 98 08 40').

U.S. Visa cards are typically personalized with the Application Label and not with the Application Preferred Name. The following discussion assumes that only the Application Label is available, but the Application Preferred Name may be used as an alternative to the Application Label as described in Section 3.3.7: Application Label and Application Preferred Name. Note also that merchants may choose to offer enhanced descriptors for debit applications as further described in Section 4.4.2 of the Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide.

Background

To support debit routing, U.S. Covered Visa Debit Cards* will be issued with both the Visa AID and the Visa U.S. Common Debit AID and both AIDs may be present in U.S. terminals. When the Visa U.S. Common Debit AID is the AID selected for the transaction, U.S. merchants and acquirers can use BIN routing logic to route these transactions to the appropriate debit network. When the Visa AID is selected, the transaction must be routed to Visa.

Options for Application Selection, Funding Selection, and CVM Selection

Per Basic EMV Application Selection processing, terminals may provide cardholders with the ability to select which application they want to use on a given transaction by building a Candidate List of all mutually supported applications and then displaying them to the cardholder for selection. This terminal selection can be customized to meet merchant preferences in the U.S.

For U.S. Covered Visa Debit Cards, merchants have flexibility to use either the Visa U.S. Common Debit AID or the Visa AID. Application Selection (including the display of an Application Selection screen) is not required by Visa for debit functionality on U.S. Covered Visa Debit Cards. Merchants are not required to use the Visa AID, and may route U.S. debit transactions using the Visa U.S. Common Debit AID exclusively if they so choose by deploying specific logic in their readers/terminals to ensure the Visa U.S. Common Debit AID is used. See Special Application Selection Logic on the next page.

---

* U.S. Covered Visa Debit Card – A Visa U.S. debit card as defined in the Visa Rules for debit and prepaid products covered by the unaffiliated network and routing requirements of the Dodd-Frank Act and Federal Reserve Board Regulation II.

Card Acceptance Guidelines for Visa Merchants

If a customer presents a U.S. Covered Visa Debit Card with multiple funding sources (e.g., credit and debit applications), merchants may present screens to enable the cardholder to select a funding source. Any such screens should clearly identify the source of funds to avoid cardholder confusion, but merchants are not required to display debit AID selection screens or labels as part of that cardholder funding selection process.

In some implementations, unless modified by the merchant, the terminal will apply U.S.-specific Application Selection logic, which may result in auto-selection of the application.

Merchants can promote their preferred verification method, including discouraging the use of signature. Where merchants automatically prompt for PIN on card present transactions, they must minimally ensure that a cardholder presenting a Visa Debit card for payment can originate a transaction using a signature (or no CVM), even if the cardholder is prompted or steered to enter a PIN.

Recommended PIN opt-out options include:

- Displaying a 'signature' button on the PIN prompt screen

- Allowing the cardholder to use the 'cancel' button to opt out of PIN prompt after clearly explaining to the cardholder how to opt out

- Using "credit" and "debit" buttons or labels with "credit" used to indicate cardholder preference to opt-out of entering a PIN and "debit" used to indicate cardholder preference to enter a PIN just as those terms were frequently used in the pre-EMV environment

Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."

Note: There are many options for how to offer PIN opt-out in a way that is transparent and consumer friendly. Cardholders can be confused by opt-out processes that utilize unlabeled terminal buttons to effect the opt-out (e.g., pushing the red button or the green button with no label or explanation). Merchants customizing their terminals to implement PIN opt-out must minimally ensure that a cardholder presenting a Visa Debit card for payment can originate a transaction using a signature (or "no CVM") even if the cardholder is prompted or steered to enter a PIN.

Other Approaches

This section outlines other possible approaches that are part of EMV processing.

Implementation of any of these alternative approaches is optional. Merchants may route all debit transactions from U.S. Covered Visa Debit Cards to the Visa U.S. Common Debit AID using special terminal logic, if they so desire. See Special Application Selection Logic.

Select Application with Highest Priority

Cardholder Selection may be inherently impractical in environments such as road tolls or transit. In these environments, the terminal can follow basic EMV processing to build the Candidate List and then automatically select the application with the highest priority (as defined by the issuer in the card's Application Priority Indicator). If the Visa AID is selected as the highest priority application, the transaction will be routed to Visa (transactions initiated with the Visa AID must be routed to a Visa network).

Special Application Selection Logic

Another approach is for the terminal to identify cards that contain both the Visa AID and the Visa U.S. Common Debit AID and eliminate one of the AIDs from the Candidate List (when these AIDs share the same funding source ["debit pairs"]). The remaining AID can then be used for routing purposes. This approach, and other options, are discussed in more detail in Section 4.4 and Appendices D and E of the *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide.*

To clarify, for U.S. Covered Visa Debit Cards, merchants have flexibility to use either the Visa U.S. Common Debit AID or the Visa AID. Merchants are not required to use the Visa AID, and may route U.S. Debit transactions using the Common AID exclusively if they so choose. If a customer presents a U.S. Covered Visa Debit Card with multiple funding sources (e.g., credit and debit applications), merchants may present screens to enable the cardholder to select a funding source. Any such screens should clearly identify the source of funds to avoid cardholder confusion, but merchants are not required to display debit AID selection screens or labels as part of that cardholder funding selection process.

Application Selection for Contactless Transactions and the Visa U.S. Common Debit AID

Contactless transactions do not support Cardholder Selection in the same way as contact chip transactions due to the minimal interaction between the contactless reader and the consumer device. The default AID to be selected will normally be the highest priority AID (as identified by the issuer or consumer) on the consumer device. So, if merchants wish to preserve their routing choice for debit functionality or offer additional options (e.g., cash-back), they must override the default selection, preselect the AID, and should preselect the Visa U.S. Common Debit AID. In other words, contactless transactions can ultimately be routed over the Visa U.S. Common Debit AID to the same extent as transactions initiated using other methods, but custom logic will be required.

This approach is discussed in more detail in Section 4.5 and Appendices D and E of the *Visa Smart Debit/ Credit and Visa payWave U.S. Acquirer Implementation Guide.*

Note: Because MSD processing is functionally equivalent to magnetic-stripe processing (though with the enhanced security of dCVV or CVN 17) and does not rely on the AID selected for routing purposes, routing flexibility for MSD transactions can be accomplished through the use of BIN routing logic.

Assumptions for EMV Processing Approaches

1. U.S. Covered Visa Debit Cards will contain a Visa U.S. Common Debit AID in addition to the Visa AID. Technically, this assumption is per BIN/PAN. This assumption is likely to remain true for some time (i.e., a given card will only have one source of debit funding).

2. A card may contain both credit and debit functionality. This will be represented by a Visa AID connected to the credit function, and a debit pair consisting of a Visa AID and a Visa U.S. Common Debit AID both connected to a common source of debit funding. Removal of one of the AIDs of the debit pair from the Candidate List will result in two eligible AIDs. Either the highest priority AID can be selected to initiate the transaction or the two AIDs can be presented to the cardholder for selection. Merchants that wish to maintain routing flexibility will need to deploy specific logic in their readers/ terminals to ensure the Visa U.S. Common Debit AID is used for debit functionality, in addition to the non-paired Visa AID for credit functionality.

3. The terminal must pass the AID (contained in the DF Name, Tag '84') used to initiate the transaction to the acquirer or other routing entity in the transaction message to enable the acquirer or other routing entities to perform appropriate routing.

U.S. Territories and Protectorates

If there is a business need in a U.S. Territory to support the Visa U.S. Common Debit AID, the terminal should set the Terminal Country Code (Tag '9F 1A') to '08 40' for the *Visa U.S. Common Debit AID only*. This will allow acceptance of the Visa U.S. Common Debit AID.

Ensuring Merchant Name and Merchant Category Code (MCC) Accuracy

How you identify your merchant business when you first sign up with your acquirer has a lot to do with your payment processing performance success, as well as your bottom line. Merchant name and MCC description clarity and accuracy are key to avoiding cardholder transaction recognition issues and misclassification of the nature of your business. The following practices can assist you in properly setting up your merchant business.

Merchant Name

The merchant name is the single most important factor in cardholder recognition of transactions. Therefore, it is critical that the merchant name, while reflecting the merchant's "Doing Business As" (DBA) name, also be clearly identifiable to the cardholder. This can minimize copy requests resulting from unrecognizable merchant descriptors.

Merchant applications typically list the merchant name as the merchant DBA. This may differ from the legal name (which can represent the corporate owner or parent company), and may differ from the owner's name which, for sole proprietorships, may reflect the business owner.

- Keep in mind that the purpose of the merchant name is to identify the merchant to the cardholder.
- Work with your acquirer to ensure your name is clear and discernible to cardholders when they read their statement.
- To verify that you are using the merchant name that is most recognizable to the cardholder, compare the merchant name that you want to use to:
  - Signage in the site photo
  - Advertisements or brochures, **and/or**
  - A telephone directory listing

MCC Descriptor

The MCC is a four-digit number assigned to describe a merchant's primary business based on annual sales volume. When an accurate MCC is assigned, it assists in the analysis of merchant sales, performance, assessment of levels of risk, and the development of programs that are the most useful to clients, merchants, and cardholders. MCC's can also be used to help in recognition of a transaction if the merchant name is not familiar to the cardholder. This can also prevent request for copy.

> Cardholder rewards are also dependent on the correct MCC.

SECTION 2
Card-Present Transactions

What's Covered

- Doing It Right at the Point of Sale
- Visa Card Features and Security Elements
- Authorization
- Cardholder Verification and Identification
- Suspicious Behavior
- Skimming
- Recovered Cards
- Visa Easy Payment Service Transactions

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. Merchants should program their terminals so that sales associates can follow the prompts and properly process the transaction.
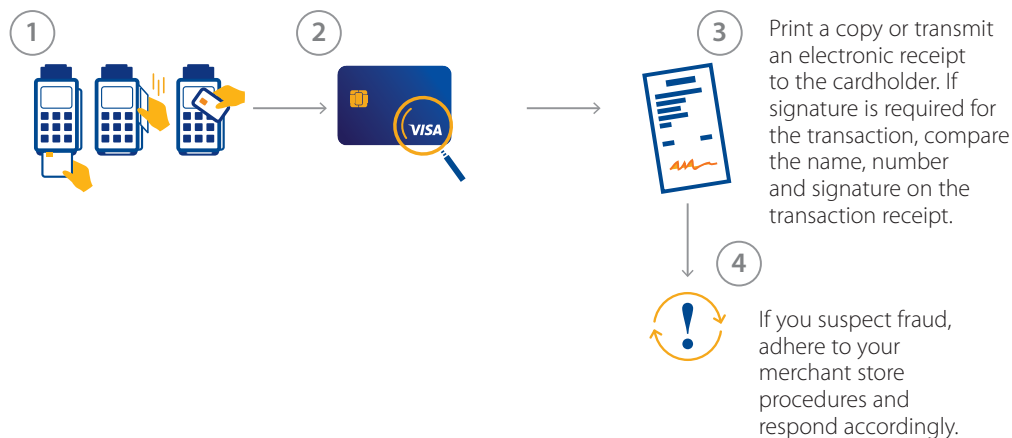
The following illustrations provide an overview of the card acceptance steps that should be followed at a point of sale (POS) terminal. Each step is explained in greater detail in this section.

Card Acceptance Processing Flow

A chip card is a plastic payment card with a microchip that is extraordinarily difficult to copy and re-use. Migrations to EMV* chip have proven the value of chip cards at reducing counterfeit fraud. The use of stronger authentication methods and unique transaction elements make chip card account data less attractive to steal, and render it nearly impossible to commit card-present counterfeit fraud.

Swipe through a magnetic card reader, wave the card in front of a Visa payWave contactless payment terminal, or insert the card into a chip-reading device** 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.

1

2

3 Print a copy or transmit an electronic receipt to the cardholder. If signature is required for the transaction, compare the name, number and signature on the transaction receipt.

4

If you suspect fraud, adhere to your merchant store procedures and respond accordingly.

* EMV is a global standard for inter-operation of chip cards, ATMs and POS terminals for authenticating credit and debit card transactions.

** 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 magnetic-stripe. The card should remain in the terminal until instructed to remove the card by the chip-reading device.

EMV Liability Shift

The EMV Liability Shift applies to qualifying transactions, as follows:

Region	Transactions in EMV Liability Shift effective before 1 October 2015	Transactions in EMV Liability Shift effective 1 October 2015	Transactions in EMV Liability Shift effective 1 October 2017
AP Region	All domestic, intraregional, and interregional[1] counterfeit POS Transactions, except Domestic Transactions in China and Japan. In addition, for Australia and New Zealand only, all domestic, intraregional,[2] and interregional[1] counterfeit ATM Transactions.	All domestic, intraregional, and interregional[1] counterfeit POS Transactions, except Domestic Transactions in China. All domestic, intraregional, and interregional[1] counterfeit ATM Transactions, except China, India, Japan, and Thailand.	All domestic, intraregional, and interregional counterfeit POS and ATM Transactions, except Domestic Transactions in China.
Canada Region	All domestic and interregional[1] POS and ATM Transactions[3]		
CEMEA Region[4]	All domestic, intraregional, and interregional[1] POS and ATM Transactions[3]		
LAC Region	All domestic,[5] intraregional and interregional[1] POS and ATM Transactions[3]		
US Region	Not applicable	All domestic and interregional[1] counterfeit POS Transactions, except Transactions at Automated Fuel Dispensers.	All domestic and interregional counterfeit POS and ATM Transactions.[6]
Visa Europe	All domestic, intraregional, and interregional[1] POS and ATM Transactions[3]		

[1] Among Visa Regions and individual countries participating in the EMV Liability Shift.
[2] Between Australia and New Zealand.
[3] Counterfeit, lost, stolen, and "not received item" (NRI) fraud only.
[4] Including Afghanistan and Pakistan.
[5] Except for fraudulent qualifying domestic Visa Easy Payment Service Transactions completed with a lost or stolen Card or "not received item" (NRI).
[6] U.S. Domestic AFD Liability shift delayed to 1 October 2020.

Lost/Stolen Liability Shift

To help improve cross-border acceptance of U.S.-issued chip cards and provide a more consistent experience for cardholders, Visa revised the liability for some transactions at unattended terminals (ATMs excluded), regardless of the cardholder verification method (CVM) used. In addition, Visa requires certain unattended terminals (ATMs excluded) to allow online-authorized chip transactions without a CVM. Accordingly, the following revisions and requirements for fraud liability and terminals apply:

• **Effective 1 April 2014**, issuers are liable for all online-authorized fraudulent chip-transactions (contact and contactless) made at an unattended terminal (ATMs excluded) that supports the processing of transactions without a CVM. In addition, all newly deployed online-capable, chip-enabled (contact

and contactless) unattended terminals (ATMs excluded) that are not replacement terminals must support the processing of transactions without a CVM.

- **Effective 1 July 2015**, all online-capable, chip-enabled (contact and contactless) unattended terminals (ATMs excluded) must support the processing of transactions without a CVM.

Visa's Global POS Counterfeit Liability Shift

Visa's global POS Liability Shift is important to all key stakeholders in the payment industry because it encourages a "chip-on-chip" transaction (i.e., a chip card read by a chip terminal) that provides dynamic authentication data.

This, in turn, helps to better protect all parties. With this Liability Shift comes a set of rules for determining who holds the liability for a counterfeit point-of- sale transaction. Under these rules, the party that is the cause of a chip transaction not occurring, either the issuer or acquirer, will be held financially responsible if the transaction is later determined to be counterfeit fraud.

- Issuers assume counterfeit fraud-related liability for non-chip cards at any type of terminal.
- Acquirers assume counterfeit liability if a chip card is presented at a non-chip terminal.

Handling Visa payWave Transactions

Visa payWave uses the latest technology to send card data wirelessly to a terminal reader. When the merchant terminal is enabled with contactless technology, the transaction process is quick and simple.

1. Customer looks for Visa payWave symbol at checkout.
2. Customer waves card or contactless device (e.g., mobile phone) in front of the secure reader and terminal light and sound indicates card has been read.

Insert Chip Card

In most point point-of-sale situations, the cardholder, not the merchant, inserts the card 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*.

Merchants are encouraged to ask the cardholder to:

- **Insert** the card into the chip-reading device. If the card is swiped first, the terminal will read the service code and display a prompt 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.
- Make sure the card is inserted in the chip-reading device until instructed to remove the card by the chip-reading device.
- The card should not be swiped unless instructed to do so on the terminal screen.
- 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.

---

* 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 magnetic-stripe. The card should remain in the terminal until instructed to remove the card by the chip-reading device.

     – If the card and chip-reading device have more than one application in common, one of the EMV prescribed methods application selection must be used. In the US, merchants may use one of the methods of application selection as described in the US AIG.

     – Remind customer to remove the card from the device.

If the Terminal Cannot Read the Chip

If the chip-reading device cannot read the chip on the card, you should follow "fallback" acceptance procedures. If the chip cannot be read, the terminal should first fallback to magnetic stripe, only if the magnetic stripe cannot be read should key entered take place. Key entered transactions should be the last option. Key entered transaction are addressed in more detail in the following section.

Because the fallback transaction is swiped or keyed, the normal rules of transaction processing for zero floor limit transactions, as applicable, will come into play meaning that a signature will be required, without an option to capture PIN, for key-entered transactions, manual imprints will be required. Merchants should not force a fallback transaction, and are more likely to see declines for fallback transactions, than for a valid chip card transaction. Ensure staff are trained to follow the prompts on the terminal to avoid higher levels of key-entered transactions. The liability shift does not impact key entered rules as the counterfeit liability remains with the party that has not invested in chip technology.

Swiping the Stripe

On the back of every Visa card, you'll find a magnetic-stripe. It contains the cardholder's name, card account number, and expiration date, as well as special security information designed to help detect counterfeit cards. When the magnetic-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.

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, or there is a power outage.

- 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 26 in this section.)

- If the problem appears to be with the magnetic-stripe, follow your merchant 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.

(US) U.S. merchants who work in the face-to-face sales environment may include CVV2 in the authorization request for U.S. domestic key-entered transactions in lieu of taking a manual card imprint. The CVV2 with Magnetic-Stripe Failures process is applicable to all card products when the magnetic-stripe fails at the point of sale (e.g., embossed cards, unembossed cards, vertical cards and cards with customized designs).

- If an unembossed card will not swipe and the chip cannot be read, you should ask for another form of payment. Do not manually key enter unembossed cards (unless you participate in the CVV2 with Magnetic-Stripe Failures process), or write the account number on a paper draft. A marked paper draft will not protect a merchant against chargebacks.

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.

How to Minimize Key-Entered Transactions

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

Pinpoint Areas with High Key-Entry 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 most common cause of fallback is by terminals that are coded incorrectly as being chip activated, when they are only capable of reading magnetic-stripe cards. The following chart summarizes the most common reasons for high key-entry rates and provides possible solutions.

Key-Entry Cause	Solution
Damaged Magnetic-Stripe Readers or Chip-Reading Device	Check magnetic-stripe readers or chip-reading devices regularly to make sure they are working.
Dirty Magnetic-Stripe Readers or Chip-Reading Device	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.
Magnetic-Stripe Reader or Chip-Reading Device Obstructions	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.
Spilled Food or Drink	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.
Anti-Theft Devices that Damage Magnetic-Stripes	Keep magnetic anti-theft deactivation devices away from any counter area where customers might place their cards. These devices can erase a card's magnetic-stripe.
Improper Card Swiping	• Swipe the card in one quick, smooth motion. • Never swipe a card back and forth. • Never swipe a card at an angle. This may cause a faulty reading.
Improper Card Insertion	• Never insert a card at an angle.
Technical Difficulties (Card or Terminal)	Report repeated card failures to your acquirer for further investigation/action.
Untrained Staff	• Make sure your staff is aware of proper acceptance procedures. • Request training and/or best practices material from your acquirer.

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 swipe, insert, or wave 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.

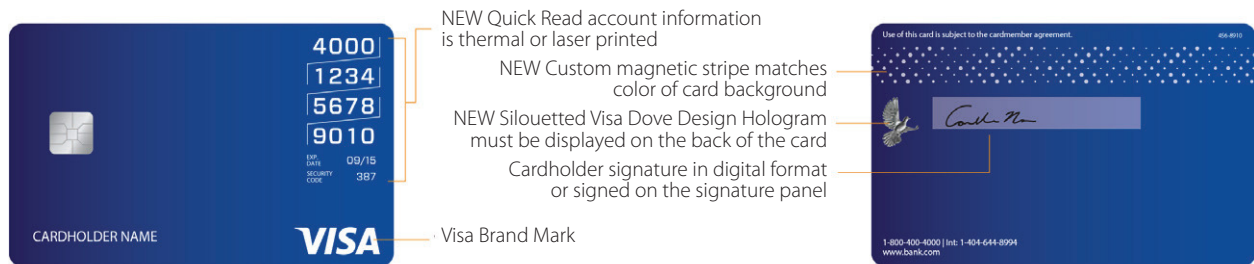## What to Look For On All Visa Cards

Visa Brand Mark Card Security Features

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

Chip may appear on the card front

Dove Hologram may appear on the front or back of the card

Visa Brand mark may be placed in the upper left, upper right, or lower right corner of the card

Ultraviolet V is viable over the Visa logo when the card is placed under an ultraviolet light

Four to Six Digit Bank Identification Number (BIN) must be printed directly below the account number and must match exactly with the first four digits of the account number

Expiration or "Good Thru" dates should appear below the account number

The Signature Panel must appear on the back of the card and be signed

Magnetic Stripe is encoded with the card's identifying information

The Mini-Dove Design Hologram may appear on the back anywhere within the outlined areas shown here. The three-dimensional dove hologram should appear to move as you tilt the card.

The Mini-Dove Design Hologram may appear on the back anywhere within the outlined areas shown here. The three-dimensional dove hologram should appear to move as you tilt the card.

Card Verification Value (CVV)* is a unique three-digit code on the magnetic-stripe of all valid cards

* In certain markets, CVV2 is required to be present for all card-absent transactions. Also, U.S. merchants who work in the face-to-face sales environment may include (CVV2) in the authorization request for U.S. domestic key-entered transactions in lieu of taking a manual card imprint.

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, insert, or wave 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 manual card imprint. A merchant should not attempt to hand-write receipts or key-enter the account number for unembossed cards.

NEW Quick Read account information is thermal or laser printed

NEW Custom magnetic stripe matches color of card background

NEW Silouetted Visa Dove Design Hologram must be displayed on the back of the card

Cardholder signature in digital format or signed on the signature panel

Visa Brand Mark

Visa Mini Card

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

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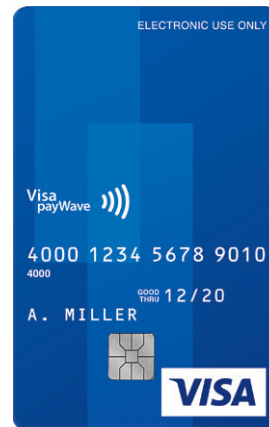
This card has a vertical orientation and account information is laser printed on the card, not embossed. It includes a magnetic-stripe just like its embossed counterpart, and a card verification code on the back.

When Something Doesn't Look Right

If any of the Visa card security features are missing or look altered, adhere to your merchant store procedures and respond accordingly.

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).

Response	Meaning
Approved	Card issuer approves the transaction. This is the most common response.
Declined or Card Not Accepted	Card issuer does not approve the transaction. The transaction should not be completed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account.
Call, Call Center, or Referrals	Card issuer needs more information before approving the sale. You should call your authorization center and follow whatever instructions you are given. In most cases, an authorization Agent will ask to speak directly with the cardholder or will instruct you to check the cardholder's identification.
Pick Up	Card issuer wants to recover the card. Do not complete the transaction. Inform the customer that you have been instructed to keep the card, and ask for an alternative form of payment. If you feel uncomfortable, simply return the card to the cardholder.

> For more information on about card pick up and recovery, see *Recovered Cards* on page 37 in this section.

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. The card and terminal will automatically determine which is appropriate.
- Not seek the authorization, but compare the card number to the current Card Recovery Bulletin (CRB). **This action is not required for merchants using chip terminals.**

> For many transactions, the floor limit is zero. This means the merchant will be liable for chargeback No-Authorization if it does not obtain an online authorization approval.

> The Card Recovery Bulletin (CRB) is an International list of lost/stolen, counterfeit, and other cards that card issuers have listed for pickup. For more information about the CRB, contact your acquirer.
>
> (AP) (Can) (CEMEA) (LAC)

CRB Actions

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.

Floor Limits and Required Authorization

For some transactions, a merchant is required to seek online authorization. These are listed in the Visa Rules. In addition, Visa has floor limits for particular countries, MCCs or transaction types. If a transaction is above the floor limit, the merchant faces liability from No_authorization if it fails to obtain online authorization.

Note: The embedded chip on the card contains issuer-defined parameters that guide the acceptance procedure in a 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.

Tip Authorizations

See *Tips* on page 12 in this guide for further details.

Split-Tender Transactions

Merchants are encouraged to accept a split-tender transaction as an alternative to a decline when the available card balance is not sufficient to approve a transaction in full. 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

(AP)
(Can)
(CEMEA)
(US)

A Partial Authorization enables participating merchants to receive an approval for a partial amount of a transaction (i.e., the amount available on the card) when the amount in the original authorization request exceeds the available card balance. The merchant may then request another form of payment to cover the remaining transaction amount. This service provides an alternative to receiving a decline when the available card balance is not sufficient to approve a transaction in full. The issuer is able to return an authorization response with an approval for a portion of the original amount requested, enabling the remainder of the transaction amount to be paid by other means using split tender functionality, where applicable.

All cashback merchants and AFD transactions (U.S. only) must support Visa Partial Authorization.

Prepaid Card Acceptance

Prepaid product cardholders often do not know whether their available balance is enough to complete a point-of-sale purchase. Without this information, merchants can experience lost sales or excessive time spent at checkout trying to determine if a sale will be approved.

To streamline the checkout process and make sure that prepaid cardholders can use the remaining available funds, Visa has developed three optional point-of-sale solutions for merchants worldwide.

- **Visa Point of Sale Balance Inquiry Service** provides a participating merchant with the capability to give cardholders available balance information on non-reloadable Visa Gift and Incentive cards via a stand-alone terminal, even if a purchase is not involved. U.S. issuers of non-reloadable prepaid cards are required to support the Balance Inquiry Service.

- **Visa Point of Sale Balance Return Service** offers the merchant the ability to provide available balance information printed on a cardholder's receipt at the conclusion of a transaction a the point-of-sale. U.S. issuers of non-reloadable prepaid cards are required to support the Balance Return Service.

- **Visa Partial Authorization**** (See description above).

  Implementation of Visa Partial Authorization is preferred and should be enabled by merchants if their payment processing systems can support it. Merchants who cannot support Visa Partial Authorization due to system limitations, should implement the Visa Point of Sale Balance Inquiry or Balance Return Services. These services are especially useful for split tender transactions that involve non-reloadable prepaid card products.

* Floor limits apply to all regions, except the U.S.

** Partial Authorization is not available in LAC.

Cardholder Verification and Identification

The final step in the card acceptance process for transactions is to verify the cardholder's signature, PIN or other methods as required in the Visa Rules. Visa supports a range of cardholder verification methods including signature, PIN, and PIN-less methods such as CDCVM (Consumer Device Cardholder Verification Method).

1. **Signature** – Verify that the signature on the Card matches the signature on the Transaction Receipt and on any identification required and presented

2. **PIN** – Verification using an acceptance device with electronic capability accepts a cardholder's PIN rather than a signature. The merchant must not ask the cardholder to reveal the PIN.

3. **CDCVM** – a verification that is performed on the consumer's payment device, independent from the reader (such as a mobile phone).

Checking Signatures

All attended devices must support signature cardholder verification. 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, check the two signatures closely for any obvious inconsistencies in spelling or handwriting.

- 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.

For suspicious or non-matching signatures, adhere to your merchant store procedures and respond accordingly.

When a Signature Line is Not Present

When a transaction is PIN or CDCVM verified, 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 a different signed Visa card.**

> 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, follow recommended steps listed above under *Unsigned Cards.*

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.

PIN Entry

PIN verification is performed by verifying the PIN entered at the point of transaction, either online by the issuer or offline using a chip card. Using either method, if the PINs match, the cardholder's identity is deemed to have been correctly verified.

CDCVM

Under Visa Rules, fingerprint and passcode technology may be an acceptable form of Cardholder Verification Method (CVM) for Visa transactions initiated on a mobile device, provided that your NFC terminal supports it (i.e., the contactless reader meets VCPS specification version 2.1 or above/EMVCo Contactless Kernel 3 version 2.2 or above, and is processed using the QVSDC transaction flow). If the NFC terminal does not meet the required specification, you are required to request a cardholder signature or PIN to complete the purchase. Merchants are reminded that a consumer's signature or PIN may still be required if the NFC terminal at the merchant location does not support VCPS version 2.1 or above/EMVCo Contactless Kernel 3 version 2.2 or above and is processed using the QVSDC transaction flow.

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, adhere to your merchant store procedures and respond accordingly.

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.

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

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.
    - Apparent tampering with the in-store point-of-sale devices (scratches, color changes, devices attached to point-of-sale (POS) cables, etc.)
- Ensure that card data is protected in accordance with the PCI DSS requirements 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**.

Ensuring Point-of-Sale Devices Security

By keeping your equipment safe and your staff trained — and by knowing what to do if there's a problem — you can prevent your business from falling prey to criminals out to steal payment card data and PINs from POS terminals.

Consider applying some of these key best practices to prevent thieves from tampering from your POS terminals.

- Track and monitor all POS terminals that accept Visa cards.
- Check for simple abnormalities. A missing seal or screw, or extra wiring or holes, for instance — could be the first step to uncovering fraud. You should also look out for added labels, decals or other materials that may be masking damage inflicted by tampering.
- Routinely inspect POS terminals and PIN-entry devices (PEDs) and secure terminals to counters to prevent removal.
- Secure your POS devices.

- **Where practical, anchor your equipment with secure stands, tethers, or alarms to prevent devices from being replaced by substitutes and reduce the chance of tampering.** Connector cables should also be safeguarded. Whenever possible, protect them by using a conduit, or contain them within a secure structure.

- **Install closed-circuit cameras to monitor all POS terminals.** Position them so that they do not record customers' PIN-entry process.

> For additional tips and best practices on how to keep your point-of-sale terminals secure, refer to *Protect Your Merchant Terminals from Illegal Tampering*. For a copy of this document, visit <u>visa.com</u> or contact your acquirer.

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 26 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 through 25 of this document.)
- You receive a pick-up response when a card has been swiped for electronic authorization.

Card Recovery Procedures

The following card recovery procedures apply to all Visa credit, debit, prepaid and Visa 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 Easy Payment Service Transactions

What is VEPS?

Visa Easy Payment Service (VEPS)* is a program that allows merchants to eliminate cardholder verification and receipts on qualifying low value transactions to help deliver greater efficiency and convenience to both merchants and cardholders.

The VEPS program provides face-to-face merchants with the ability to accept Visa card for purchases without requiring a cardholder verification and foregoing a receipt unless requested by the cardholder. This program has the potential to increase speed at the point-of-sale (POS), 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. Transactions that cannot be electronically read at the POS are not eligible for the VEPS program. You must continue to obtain a cardholder signature on transactions that are key-entered or manually processed at POS.

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

VEPS 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.

* Specific country/regional requirements are defined in the Visa Rules.

How to Process a VEPS Transaction

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

Merchant Category Codes (MCCs) Excluded from VEPS

Table: MCCs Excluded from Visa Easy Payment Service Program	
4829	Wire Transfer Money Orders
5542	Automated Fuel Dispensers*
5960	Direct Marketing—Insurance Services
5962	Direct Marketing—Travel Related Arrangement Services
5964	Direct Marketing—Catalog Merchants
5965	Direct Marketing—Combination Catalog and Retail Merchants
5966	Direct Marketing—Outbound Telemarketing Merchants
5967	Direct Marketing—Inbound Telemarketing Merchants
5968	Direct Marketing—Continuity/Subscription Merchants
5969	Direct Marketing/Direct Marketers (Not elsewhere classified)
6010	Financial Institutions—Manual Cash Disbursements
6011	Financial Institutions—Automated Cash Disbursements
6012	Financial Institutions—Merchandise and Services
7995	Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks
9405	Intra-Government Purchases (Government only)
9700	International Automated Referral Service (Visa use only)
9701	Visa Credential Server (Visa use only)
9702	GCAS Emergency Services (Visa use only)
9950	Intra-Company Purchases

* In Canada, MCC 5542 is allowed to conduct contactless transactions without a Cardholder Verification Method (CVM)

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
- Split-shipment Transactions

Industry Changes

Consumers are turning to digital devices to initiate purchases leading to explosive year-over-year growth in eCommerce. Online purchases provide greater flexibility for consumers to shop. The data analytics allow consumers to compare products, features and pricing, and in some cases have instant or same day product delivery. This level of convenience is becoming more mainstream migrating consumers from traditional brick and mortar retail. Merchants are finding themselves in more situations where the card and cardholder are not present, and fraud may be especially difficult to detect transactions, so as to reduce unnecessary friction and disputes.

This section covers basic card acceptance procedures for both MO/TO and eCommerce 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 electronic commerce 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 and the name of the financial institution that issued the card.
- Also, whether the transaction is processed by phone, mail or electronic commerce, obtain proof of delivery.
- 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.

  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)**, Verified by Visa, and Visa Checkout. For more information visit www.visa.com.
- 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 eCommerce 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 eCommerce order containing an invalid or missing expiration date may indicate fraudulent use of the card.

Ask for CVV2

The Card Verification Value 2 (CVV2)* is a three-digit security number printed on the back of Visa cards on the signature panel and helps validate that a customer is in possession of the card at the time of an order. (See *Visa Card Features and Security Elements* on page 26 in *Section 2: Card-Present Transactions* of this document.)

> 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.

- You should also include one of the following CVV2* presence indicators, even if you are not including a CVV2 in your authorization request:

If:	Send this Indicator to the Card Issuer:
You have chosen not to submit CVV2	0
You included CVV2 in the authorization request	1
Cardholder has stated CVV2 is illegible	2
Cardholder has stated CVV2 is not on the card	9

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

Result:	Action:
M – Match	Complete the transaction (taking into account all transaction characteristics and any questionable data).
N – No Match**	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.
P – Not Processed	View the "Not Processed" as a technical problem or the request did not contain all the information needed to verify the CVV2 code. Resubmit the authorization request.
S – CVV2 should be on the card	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.
U – Card issuer does not participate in the CVV2 service	Evaluate all available information and decide whether to proceed with the transaction or investigate further.

- 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.

Billing Address Verification with AVS

Can

US

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 and merchant 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 and a response to the AVS information submitted.

* For more information regarding the Zero Amount Account Number Verification Service, contact your acquirer.

How to Use AVS

Can

US

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. We have seen incidents where the merchant included their own address in the AVS request. Please ensure that this is avoided as the issuer will most likely decline that transaction on account of a mismatch.

- 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 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."

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

Address Verification Results Codes

Code	Definition	Domestic Can US	International
A	Street address matches, but the ZIP code does not. Acquirer rights not implied.	✔	✔
B	Street addresses match. Postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)	✔	✔
C	Street address and postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)	✔	✔
D	Street addresses and postal codes match.		✔
F	Street address and postal code match. (Applies to U.K. only).		✔
G	Address information not verified for international transaction. Issuer is not an AVS participant, or AVS data was present in the request, but issuer did not return an AVS result, or Visa performs AVS on behalf of the issuer and there was no address record on file for the account.		✔
I	Address information not verified.		✔
M	Street address and postal code match.		✔
N	No match. Acquirer sent postal/ZIP code only, or street address only, or both postal code and street address. Also used when acquirer requests AVS, but sends no AVS data in field 123.	✔	✔
P	Postal code match. Acquirer sent both postal code and street address, but street address not verified due to incompatible formats.	✔	✔
R	Retry. System unavailable or timed out. Issuer ordinarily performs AVS, but was unavailable. The code R is used in V.I.P. when issuers are unavailable. Issuers should refrain from using this code.	✔	
S	Not applicable. If present, replaced with "U" (for domestic) or "G" (for international) by V.I.P. Available for U.S. issuers only.	✔	
U	Address not verified for domestic transaction, issuer is not an AVS participant, or AVS data was present in the request, but issuer did not return an AVS result, or Visa performs AVS on behalf of the issuer and there was no address record on file for this account.	✔	
W	Not applicable. If present, replaced with "Z" by V.I.P. Available for U.S. issuers only.	✔	
X	Not applicable. If present, replaced with "Y" by V.I.P. Available for U.S. issuers only.	✔	
Y	Street address and postal code match.	✔	
Z	Postal/ZIP code matches, street addresses does not match or street address not included in request.	✔	✔

Note: Issuers can send codes S, W, and X, but they are converted at the VisaNet Interchange Center (VIC) to G, U, Z, and Y as appropriate before the message is forward to the acquirer.

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

> If you complete a transaction for which you received an authorization approval and an AVS response of "U" (unavailable), and the transaction is later charged back to you as fraudulent, your acquirer may represent the item. U.S. card issuers must support AVS or lose their right to fraud chargebacks for card-absent transactions. Card issuers also lose fraud chargeback rights for "U" responses in CVV2* request situations.

Guidelines for Using Domestic and Cross-border AVS Result Codes

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.

U.S. Code	Int'l Code	Definition	Explanation	Action(s) to Consider
Y	D F M	Exact Match	Street address and postal code match.	Generally speaking, you will want to proceed with transactions for which you have received an authorization approval and an "exact match."
A	B	Partial Match	Street address matches, but the ZIP code does not. Acquirer rights not implied.	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.
Z	P	Partial Match	Postal/ZIP code matches; street address does not match or street address not included in request.	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 on 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.
N	N	No Match	No match. Acquirer sent postal/ZIP code only, or street address only, or both postal code and street address. Also used when acquirer requests AVS, but sends no AVS data in field 123.	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.

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).

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

International Addresses

Can

US

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)

US

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 eCommerce 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.

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

eCommerce Transactions

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.

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 email 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 email address promotes customer satisfaction.

- **Return, refund, and cancellation policy.** This policy must be clearly posted. (See *Disclosure for Card-Absent Merchants* on page 16.)

- **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 prominently display the merchant location country on the checkout page or a page leading up to it. You must also disclose the address for cardholder correspondence. Check with your acquirer to ensure your disclosure is made in accordance with the *Visa Core Rules and Visa Product and Service Rules* and local law.

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

Best Practices for Websites

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 email 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 customer's personal information or data.**

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

Your acquirer may require that your merchant website include any of the above elements.

Additional Fraud Prevention Tools for the Internet

Today's eCommerce 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 merchants with cardholder authentication on eCommerce transactions. Verified by Visa helps reduce eCommerce fraud by helping to ensure that the transaction is being initiated by the rightful owner of the Visa account. This gives merchants greater protection on eCommerce transactions.

Merchants offering Verified by Visa to their customers must incorporate a software module called a Merchant Plug-In (MPI), as part of their eCommerce server application. Merchants who opt to implement Verified by Visa must use PCI compliant vendors and payment solutions.

Fraud Screening

Today, a wide variety of fraud-screening services and practices is available to help eCommerce 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 email 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.

> **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.

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

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

Other Card-Absent Fraud Detection Tools

To supplement the effective use of your own data, Visa's fraud prevention tools, third party data feeds/ services, and fraud detection solution vendors such as CyberSource* offer a combination of leading technology and innovative tools for fraud mitigation within the various card-absent channels. These solutions are designed to help you protect your customers and brand by reducing fraud losses and making the Internet and other sales channels safer to conduct business.

CyberSource Risk Management Solutions** provide the following fraud detection for organizations of all sizes.

*   **Decision Manager (DM) and Managed Risk Services by CyberSource** enable mid-size to large companies to detect fraud more accurately, review transactions more efficiently, and improve control over fraud management practices.

*   **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. Authorize.Net AFDS is a value-added service of the Authorize.Net Payment Gateway.

> To obtain a list of third party fraud prevention solution vendors, contact your acquirer or payment processor.

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.

* CyberSource is a wholly-owned subsidiary of Visa.

** CyberSource Decision Manager and Managed Risk Services are available globally.

> 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.

Use of Other Innovative Fraud Alert Technologies

- Consider the use of Ethoca alerts for near real-time notification from card issuers regarding confirmed fraud. Through its relationships with Visa and a global network of card issuing banks, Ethoca is able to deliver cardholder confirmed data in the form of alerts to effected merchants through an easy to use portal or direct link API. Ethoca alerts are received in near real-time enabling merchants to act quickly stopping fraud and avoiding chargebacks.

- Learn more about Ethoca's platform. Visit www.ethoca.com or contact Sales at sales@ethoca.com for sales inquiries.

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.

Guidelines for eCommerce Merchants

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

Characteristics to watch out for include:

- **First-time shopper.** Criminals are always looking for new 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.
>
> (Can) (US)

- **Orders from Internet addresses that make use of free email services.** These email 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.

What To Do If You're Suspicious

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

Mail Order/Telephone Order Merchants

For suspicious MO/TO transactions, you should:

- **Ask 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.

eCommerce Merchants

For suspicious transactions, eCommerce 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 Transaction

An initial, or set-up, recurring transaction should be processed the same as any MO/TO or eCommerce 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.

When authorizing an initial recurring transaction, merchants should use the recurring indicator in the authorization request.

Setting Up Recurring Transactions by Email

Visa allows eCommerce merchants to accept an electronic record, such as an email 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.

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

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.**

- **Use AVS.**

(Can)

(US)

- **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.** As a best practice, routinely notify cardholders of regular recurring transactions 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.
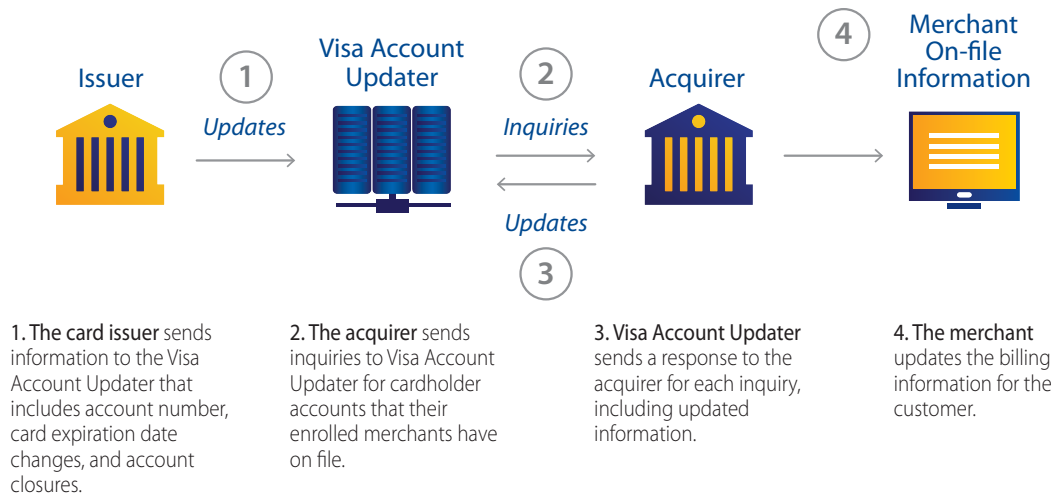
> VAU service helps ensure that merchant on-file information (cardholder account number, expiration date, status, etc.) is current. VAU allows Visa merchants, acquirers, and card issuers to electronically exchange the most current cardholder account information, without transaction or service interruption. The VAU service is available in all markets, however, usage is not mandatory.

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.

Cancelling Recurring Transactions

To cancel a recurring transaction, merchants should:

- **Check customer logs daily for cancellation or non-renewal of services paid for with a recurring transaction.** Comply with all cancellation and non-renewal requests in a timely manner and in compliance with the requirement of local laws and notify the cardholder that the recurring transaction 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.

Handling Declined Recurring Transactions

To properly handle declined recurring transaction situations, merchants should:

- Contact the cardholder to request new card number and expiration date.

- Work with the acquirer to determine if the account has been reported as fraud.

- **Work with the card issuer (through the acquirer) to determine the reason for the decline.** Any transactions that are force-posted (no attempt to authorize) may be faced with chargebacks.

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

Card Acceptance Guidelines for Visa Merchants

Split-shipment Transactions

Merchants who process card-absent transactions containing multiple items for a single order find themselves shipping multiple goods at different times and/or from multiple vendors, distribution centers and store locations. These transactions are referred to as split-shipment transactions. Merchants a re encouraged to employ the following best practices to better manage the processing of split-shipment card-absent transactions.

Merchant is unable to determine the final transaction amount because sales tax and/or shipping cost is not known at the time of purchase

Authorization:

- Authorize for the anticipated transaction amount without sales tax and/or shipping cost.

Clearing:

- If the clearing amount (transaction amount + shipping + tax) is within 15 percent variance between the original authorization amount and the clearing amount, then clear the transaction amount plus sales tax and shipping amount.

- If the clearing amount (transaction amount + shipping + tax) is greater than 15 percent variance between the authorization amount and the clearing amount:

  – Clear original transaction amount as shipped.

  – Authorize and create a new transaction for the additional amount that is above the original authorization amount.

  EXAMPLE

  Situation: Original transaction is $100 Final amount is $120 Visa Recommended

  Approach: Clear $100 and then authorize a new transaction for $20.]

DO NOT

- Clear a single final transaction amount that is greater than 15 percent of authorization amount due to tax and shipping. This can result in chargeback exposure.

Single purchase into multiple shipments

Authorization:

- Authorize for total purchase amount.

Clearing:

- For each shipment within 7 calendar days of authorization, clear each shipment amount as each item is shipped.

- Include the following fields in the clearing transactions:
  - Original Authorization Transaction ID
  - Original Authorization Code
  - Authorized Amount – Total Authorized Amount = Authorization less amount reversed
  - Multiple Clearing Sequence Number
  - Multiple Clearing Sequence Count
    Note: The Multiple Clearing Sequence Number should be populated in ascending order. That is, the first clearing transaction must have the multiple sequence number set to 01.

DO NOT

- Clear multiple shipments using original authorization without the Multiple Clearing Sequence Number/Count and/or without the original authorization transaction ID and authorization code. In some countries this can result in a higher Interchange Reimbursement Fee rate, rules violation, Processing Integrity Fees (only applicable in the U.S.), and global duplicate transaction ID fees. • Clear multiple shipments using the original authorization without including the Authorized Amount and Total Authorized Amount fields in the clearing transactions.

Customer or merchant cancels the order prior to shipment

Authorization:

- Authorize for total purchase amount.

Clearing:

- Reverse original authorization (within 72 hours).

DO NOT

- Authorize for total purchase amount, and not reverse original authorization. **In the U.S. this can result in Processing Integrity Fees and/or a rules violation.**

Order amount is adjusted prior to final shipment

Authorization:

- Authorize for original purchase amount.

Clearing: For shipment amounts < original authorization:

- If a shipment is within 7 calendar days of authorization, partially reverse the difference between the authorized amount and the shipment amount, then clear shipment amount as shipped.
- If a shipment is after 7 calendar days of authorization, first reverse the original authorization within 3 days. Then authorize for the new amount and clear the shipment amount as shipped.

Payment Card Industry Data Security Standard

What's Covered

- Payment Card Industry Data Security Standard Requirements
- Steps and Requirements for Compromised Entities

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 validation requirements vary depending on the merchant's annual card transaction volume.

Payment Card Industry Data Security Standard Requirements

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.

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 eCommerce.

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 (U.S. only). All other regions should refer to their regional sites for more information.

Secure technologies such as point-to-point encryption and tokenization, when implemented in accordance with the PCI DSS, may help simplify PCI DSS compliance. Go to www.pcissc.org for guidelines on these technologies.

Twelve Basic Requirements

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.

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

Additional information on PCI DSS can be found at www.pcissc.org.

Who Must Comply

Compliance with PCI DSS applies to any entity—meaning any merchant or service provider including Third Party Agents (TPA) and VisaNet processors—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.

Steps and Requirements for Compromised Entities

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

> 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 and 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:

US	U.S. – (650) 432-2978 or usfraudcontrol@visa.com
Can	Canada – (416) 860-3090 or CanadaInvestigations@visa.com
LAC	Latin America & Caribbean – (305) 328-1713 or LACFraudInvestigations@visa.com
AP **CEMEA**	Asia Pacific and Central and Eastern Europe, Middle East and Africa (CEMEA) – +971 4 457 7214 or VIFraudControl@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. **Review Visa's communication guideline for compromised entities on how to respond to a data breach.** There are some good basic communications principles that can be applied to most data breach situations. This guideline is intended to provide some best-practice guidance for compromised entities on how to think about, prepare for and respond to data breaches. You can download a copy of the guideline at www.visa.com in the Merchant Resource library.

6. **Provide all compromised Visa, Interlink, and Plus accounts to your acquirer or to Visa within ten 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.

7. **Within three 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 Payment Card Industry Forensic Investigator (PFI) will be initiated on the compromised entity. For the PFI listing, go to https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php for a list of approved PFIs.

Glossary

Account number	An issuer-assigned number that identifies an account in order to post a transaction.
Acquirer	A client that signs a merchant or disburses currency to a cardholder in a cash disbursement, and directly or indirectly enters the resulting transaction receipt into interchange.
Address Verification Service (AVS) (Can)	An optional VisaNet service through which a merchant can verify a cardholder's billing address before completing a transaction in a card-absent environment.
Address Verification Service (AVS) (US)	A VisaNet service through which a merchant can verify a cardholder's billing address before completing any one of the following: • A mail/phone order or eCommerce transaction where merchandise or airline tickets will be delivered to the cardholder or the cardholder's designee, or where services were purchased. • A CPS/retail key-entry transaction • A CPS/account funding transaction or CPS/eCommerce basic transaction • A CPS/eCommerce preferred retail transaction • A CPS/eCommerce preferred hotel and car rental transaction • An Automated Fuel Dispenser (AFD) transaction (ZIP only inquiry) • A face-to-face environment transaction if the merchant has been qualified by Visa to use AVS (ZIP only inquiry)
ATM	An unattended magnetic-stripe, contactless or chip-reading terminal that has electronic capability, accepts pins, and disburses currency.
Authorization	A process where an issuer, a VisaNet processor, or Visa Stand-In Processing (STIP) approves a transaction. This includes offline authorization.
Authorization Reversal	A VisaNet message that cancels an approval response previously sent through the V.I.P. System as specified in the *Visa Core Rules and Visa Product and Service Rules* and applicable VisaNet manuals. An authorization reversal may be for the full amount of the previous authorization or an amount less than the previous authorization amount.

"Call" or "Call Center" response	A response to a merchant's authorization request indicating that the card issuer needs more information about the card or cardholder before a transaction can be approved. Also called a "Referral" response.
Card acceptance procedures	The procedures a merchant or merchant employee must follow during the point-of-sale transaction to ensure that a card and cardholder are valid.
Card expiration date (Expiry)	See *"Good Thru" date*.
Cardholder	An individual who is issued and authorized to use a card or virtual account.
Card issuer	A financial institution that issues Visa cards.
Card-absent environment	An environment where a transaction is completed under both of the following conditions: • Cardholder is not present • Card is not present
Card-present environment	An environment that comprises the conditions of either the face-to-face or unattended environments.
Card Recovery Bulletin (CRB)	A directory of blocked account numbers listed on the International Exception File, intended for distribution to merchants. The Card Recovery Bulletin may take one of the following forms: • National Card Recovery Bulletin • National Card Recovery File • Regional Card Recovery File
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 Product Brand Standards**. 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 check value encoded on the magnetic-stripe of a card to validate card information during the authorization process. The card verification value is calculated from the data encoded on the magnetic-stripe using a secure cryptographic process.
Card Verification Value 2 (CVV2)*	A unique check value printed on the back of a card, which is generated using a secure cryptographic process, as specified in the *Payment Technology Standards Manual*.
Chargeback	A transaction that an issuer returns to an acquirer.

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

Chip	An electronic component designed to perform processing or memory functions.
Chip card	A card embedded with a chip that communicates information to a point-of-transaction terminal.
Chip-initiated transaction	An EMV and VIS-compliant chip card transaction that 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.
Common Purchase Point (CPP) (AP)	An individual merchant outlet where confirmed skimming has occurred on three or more account numbers either: • Within 30 calendar days • As a testing point for active account numbers
Contactless Payment Terminal (US)	A point-of-transaction terminal that reads the magnetic-stripe data on a contactless payment chip through a Visa-approved wireless interface, and that includes magnetic-stripe-reading capability.
Copy request	A retrieval request that is processed through an electronic documentation transfer method.
Credit transaction receipt	A transaction receipt evidencing a merchant's refund or price adjustment to be credited to a cardholder's account.
Counterfeit card	One of the following: • A device or instrument that is printed, embossed, or encoded so as to purport to be a card, but that is not a card because an Issuer did not authorize its printing, embossing, or encoding • An instrument that is printed with the authority of the issuer and that is subsequently embossed or encoded without the authority of the issuer • A card that an issuer has issued and that is altered or re-fabricated, except one on which the only alteration or re-fabrication comprises modification of the signature panel or cardholder signature
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 completes the transaction.

Electronic Commerce Indicator (ECI)	A value used in an eCommerce transaction to indicate the transaction's level of authentication and security, as specified in the applicable *Verified by Visa Implementation Guide*.
Exception file	A VisaNet file of account numbers that a client accesses online, for which the issuer has predetermined an authorization response. The Exception File supports:

- Stand-In Processing (STIP)
- Positive Cardholder Authorization Service (PCAS)
- Production of the Card Recovery Bulletin (CRB)

Exception file (US)	A VisaNet file of account numbers for which the issuer has predetermined an authorization response, that a client accesses online.
Expired Card	A card on which the embossed, encoded, or printed expiration date has passed.
Face-to-Face environment	An environment where a transaction is completed under all of the following conditions:

- Card or proximity payment device is present
- Cardholder is present
- Individual representing the merchant or acquirer completes the transaction

Transactions in this environment include the following:

- Retail transactions
- Manual cash disbursements
- Visa Easy Payment Service (VEPS) transactions

Transactions in this environment exclude the following:

- eCommerce transactions
- Mail/phone order transactions
- Recurring transactions
- Unattended transactions
- (US) In the U.S. Region, Installment Billing Transactions

Fallback transaction	An EMV chip card transaction initially attempted at a chip-reading device, where the device's inability to read the chip prevents the transaction from being completed using the chip card data, and the transaction is instead completed using an alternate means of data capture and transmission.

Fallback transaction
 	
(Can)
	A transaction occurring in either:
	
	• An unattended environment, regardless of whether authorization is required
	
	• A face-to-face environment between a compliant chip card and a compliant chip card reading device that is either not:
	
	   – completed as a Full Data Transaction
	   – initiated as a Full Data Transaction

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.
Floor Limit	A currency amount that Visa has established for single Transactions at specific types of Merchant Outlets and Branches, above which Online Authorization or Voice Authorization is required.
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 or printed 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 electronic commerce merchant	An eCommerce merchant identified by the Global Merchant Chargeback Monitoring Program or other Visa risk management initiatives (e.g., Merchant fraud or similar region-specific programs) that causes undue economic and goodwill damage to the Visa system.
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 client that enters into a contractual relationship with a cardholder for the issuance of one or more card products.
Key-entered transaction	A transaction that is manually keyed into a point-of-sale device. Card present key-entered transactions also require an imprint of the card and a signature, to verify that a card was present at the time of the transaction.
Magnetic-stripe	A magnetic-stripe on a card that contains the necessary information to complete a transaction.
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 environment*.
Member	Client of Visa U.S.A., Visa International, Visa Worldwide, or a customer which has entered into a Services Agreement with Visa Canada. Requirements for membership are defined in the applicable Certificate of Incorporation and Bylaws.
Merchant agreement	A contract between a merchant and an acquirer containing their respective rights, duties, and obligations for participation in the acquirer's Visa or Visa Electron Program.
Merchant Servicer (MS)	An merchant servicer stores, processes, and/or transmits Visa account numbers on behalf of a member's merchant. Function examples include providing such services as online shopping cards, gateways, hosting facilities, data storage, authorization and/or clearing and settlement messages.
Payment Card Industry Data Security Standard (PCI DSS)	A set of comprehensive requirements that define the standard of due care for protecting sensitive cardholder information.
Payment gateway	A system that provides services to eCommerce merchants for the authorization and clearing of online Visa transactions.
Personal Identification Number (PIN)	See *PIN*.
Pick-up response	An authorization response where the transaction is declined and confiscation of the card is requested.
PIN	A personal identification numeric code that identifies a cardholder in an authorization request.
Point-of-sale (POS) terminal	The electronic device used for authorizing and processing Visa card transactions at the point of sale.
Primary Account Number (PAN)	See *Account Number*.
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 client, or Visa-approved non-member acting as the Agent of a member, that provides authorization, clearing, and/or settlement services for merchants and/or members. The *Visa Core Rules and Visa Product and Service Rules* refers to three types of processors: authorizing processors, clearing processors, and V.I.P. system users. See also, *VisaNet processor*.
Recurring Transaction	Multiple transactions processed at predetermined intervals not to exceed one year between transactions, representing an agreement between a cardholder and a merchant to purchase goods or services provided over a period of time.
Recurring Transaction (US)	A transaction for which a Visa cardholder provides permission, in either written or electronic format, to a merchant to periodically charge their account number for recurring goods or services. These may include payment of recurring charges, such as insurance premiums, subscriptions, Internet service provider monthly fees, membership fees, tuition, or utility charges.
Referral Response	An authorization response where the merchant or acquirer is instructed to contact the issuer for further instructions before completing the transaction.
Representment	A clearing record that an acquirer presents to an issuer through Interchange after a chargeback.
Skimming	The replication of account information encoded on the magnetic-stripe of a valid card and its subsequent use for fraudulent transactions in which a valid authorization occurs. The account information is captured from a valid card and then re-encoded on a counterfeit card. The term "skimming" is also used to refer to any situation in which electronically transmitted or stored account data is replicated and then re-encoded on counterfeit cards or used in some other way for fraudulent transactions.
Split tender	The use of two forms of payment, or legal tender, for a single purchase. For example, when buying a big-ticket item, a cardholder might pay half by cash or check and then put the other half on his or her Visa credit card. Individual merchants may set their own policies about whether or not to accept split-tender transactions.
Third Party Agents	An entity, not defined as a VisaNet processor, that provides payment-related services, directly or indirectly, to a member and/or stores, transmits, or processes cardholder data. No financial institution eligible to become a principal member of Visa may serve as a Third Party Agent. A Third Party Agent does not include: • Financial institutions that perform agent activities • Co-branding or Affinity partners • Affinity Co-Brand Partners or Global Co-Branding Partners • Card manufacturers • Card personalizers

Third party processor	A non-member organization that performs transaction authorization and processing, account record keeping, and other day-to-day business and administrative functions for card issuers and acquirers.
Token	Tokens are surrogate values that replace Primary Account Numbers (PANs) stored electronically throughout the payments ecosystem and can be used to securely conduct payment transactions.
Transaction	The act between a cardholder and a merchant or an acquirer that results in a transaction receipt, if applicable.
Transaction receipt	A paper or electronic record of a Visa card transaction which a merchant submits to an acquirer for processing and payment. In most cases, paper drafts are now generated by a merchant's POS terminal. When a merchant fills out a draft manually, it must include an imprint of the front of the card.
Unsigned card	A seemingly valid Visa card that has not been duly signed by the legitimate cardholder. Merchants cannot accept an unsigned card until the cardholder has signed it and the signature has been checked against valid government identification, such as a driver's license or passport.
Verified by Visa	A Visa-approved authentication method based on the 3-D Secure specification.
Visa Easy Payment Service (VEPS)	Visa point-of-transaction service that permits qualified Visa Easy Payment Service merchants to process small value transactions, as specified in the *Country Level Visa Easy Payment Service Transaction Limits* without requiring a cardholder verification method or the issuance of a transaction receipt unless requested by the cardholder in accordance with the procedures specified in the *Visa Core Rules and Visa Product and Service Rules*.
Visa payWave Application	A Visa application contained on a contactless chip that enables a contactless payment transaction to be performed, as specified in the Visa contactless payment specification.
VisaNet processor	A member, or Visa-approved non-member, that is directly connected to VisaNet and that provides authorization, clearing, or settlement services to merchants and/ or members.
Voice authorization	An approval response obtained through interactive communication between an issuer and an acquirer, their VisaNet processors, or the International Automated Referral Service, through telephone or facsimile communications.
Voice Authorization Center	An operator-staffed center that handles telephone authorization requests from merchants who do not have electronic point-of-sale terminals or whose electronic terminals are temporarily not working, or who have transactions that require special assistance.

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, visit visa.com or contact your acquirer.