Visa Payment Acceptance for U.S. Quick-Service Restaurants

Important Information on Confidentiality and Copyright

Note: This document is a supplement of the *Visa Core Rules and Visa Product and Service Rules*. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Core Rules and Visa Product and Service Rules, the *Visa Core Rules and Visa Product and Service Rules* shall govern and control.

Contents

About This Guide

Who Should Use This Guide

The information contained in the *Visa Payment Acceptance Best Practices for U.S. Quick-Service Restaurants* guide is geared toward the actions and decisions most pertinent to quick-service restaurants and operators in the U.S. It also includes best practices and on-the-job support tools for managers and employees.

Background

Card acceptance is instrumental in operating a successful quick-service restaurant business. More than ever, consumers want convenient, efficient, and easy-to-use services when making purchases at quick-service food establishments. For today's quick-service restaurant, card acceptance helps:

- Drive higher purchase sizes
- Speed up the transaction process for customers, and
- Serve as a valuable means to retain customer loyalty

In addition to these opportunities in the quick-service segment, card acceptance brings with it certain responsibilities and investment decisions, including the need to carefully balance risk and cost mitigation with a positive customer experience.

Visa Card Benefits

Visa cards offer many tangible benefits to quick-service restaurants by enabling them to:

- Speed transaction times and serve more customers,
- Reduce opportunities for theft, and
- Provide a more pleasurable experience for the customer.

Quick-service retail (QSR) merchants in the U.S. have a number of choices when it comes to deciding how a payment transaction should be incorporated into the customer's broader sales experience. This guide showcases the decisions and options required to operate a successful business.

Guide Purpose

The *Visa Payment Acceptance Best Practices for U.S. Quick-Service Restaurants* guide provides optimal ways to process card transactions and manage the risks posed by card payments in the quick-service restaurant segment.[1]

The guide offers a set of recommended best practices for:

- Processing authorization requests and transaction data
- Chip and contactless implementation, acceptance, and terminal testing and configuration
- Monitoring interchange and controlling downgrades
- Diagnosing and dealing with higher than acceptable key-entry or fallback rates
- Understanding Visa Easy Payment Service (VEPS) and CPS retail program qualification
- Accepting prepaid cards; handling partial authorizations
- Applying fraud-mitigation tools to address high-risk transactions or suspicious circumstances
- Applying fraud controls such as Address Verification Service (AVS) and velocity controls
- Minimizing risk of loss from chargebacks
- Ensuring compliance with Payment Card Industry Data Security Standards (PCI DSS)
- Implementing EMV Chip

Guide Focus

Given the zero floor limit in the U.S. payment environment, the majority of transactions are authorized online. This guide focuses solely on the implementation requirements relating to online-only configured terminals and does not include offline functionality.

[1] Note: Merchants are solely responsible for their decisions whether and how to implement these recommended best practices. Results from implementing the best practices are not guaranteed, and may differ from merchant to merchant.

How This Guide Is Organized

The guide is divided into three sections.

Section I. Visa Acceptance in the Card-Present Environment

Card-Present Transactions offers a general overview of a quick-service merchants' payment acceptance environment, including:

- Acceptance of magnetic-stripe, chip, and contactless transactions
- Transaction Flow
- Deferred or delayed authorization
- Contactless reader placement
- Pin-less payment brand acceptance
- Terminal branding
- PIN Security
- Visa Easy Payment Service (VEPS)
- Fraud and chargeback mitigation
- CPS Interchange Qualification

Section II. Visa Acceptance in the Card-Absent Environment

Card-Absent Transactions offers an overview of ecommerce, mail order/telephone order, and mobile app transactions, including:

- Card acceptance
- Transaction flows
- Fraud-mitigation tools
- Chargeback mitigation
- CPS Interchange Qualification

Section III. Important Information for Both Card-Present and Card-Absent Environments

This section offers information that applies to all acceptance environments

- Special Authorization Processes
- Interchange Overview
- Cardholder Data Security
- Compelling Evidence in the Dispute-Resolution Process

Section I.
Visa Acceptance in the Card-Present Environment

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.

Magnetic-Stripe and Chip Card Acceptance

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.

- Magnetic-Stripe Card Acceptance Process
- Chip Card Acceptance Process
- Contactless Acceptance Process

MAGNETIC-STRIPE CARD ACCEPTANCE PROCESS

1. Swipe through a magnetic-card reader to request the transaction authorization.

2. The card and point-of-sale device work together to determine the appropriate cardholder or verification method for the transaction, either signature, PIN, or Visa Easy Payment Service (VEPS).

   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.

3. Obtain authorization and, if required, get the cardholder signature[2] on the transaction receipt. Print a copy or transmit an electronic receipt to the cardholder.

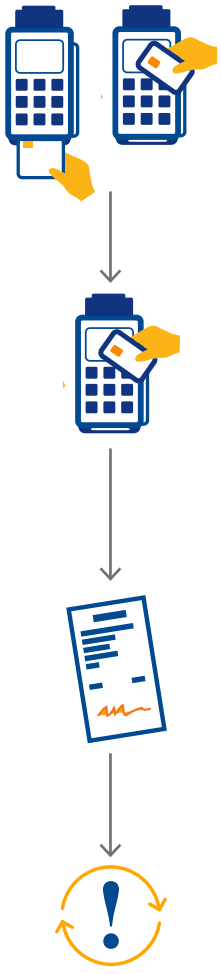
4. If signature is required for the transaction, compare the name, number and signature on the transaction receipt.

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

[2] The cardholder signature is not required if the transaction is PIN-Verified, processed with Visa Easy Payment Service (VEPS), or with some Visa payWave transactions.

CHIP CARD AND CONTACTLESS ACCEPTANCE PROCESS

A chip card is a plastic payment card with a microchip that is extraordinarily difficult to duplicate. International market migrations to EMV[3] 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 counterfeit fraud.



1. Dip the card into a chip-reading device[4] or wave the card in front of a Visa payWave reader to request the transaction authorization.

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

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

3. If the transaction has been PIN-verified, there is no need for a signature.

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

4. If you suspect fraud, adhere to your merchant store procedures and respond accordingly.[5]If you suspect fraud, adhere to your merchant store procedures and respond accordingly.

[3] EMV stands for Europay, MasterCard and Visa, a global standard for inter-operation of chip cards, ATMs, and POS terminals for authenticating credit and debit card transactions.

[4] Many Visa cards are embedded with a chip Many Visa cards are embedded with a chip. When used at a chip enabled POS terminal, the terminal will automatically prompt for the chip card to be "dipped," instead of "swiped" using the magnetic stripe.

[5] Some chip-reading devices support a "merchant suspicious" indicator on the authorization.

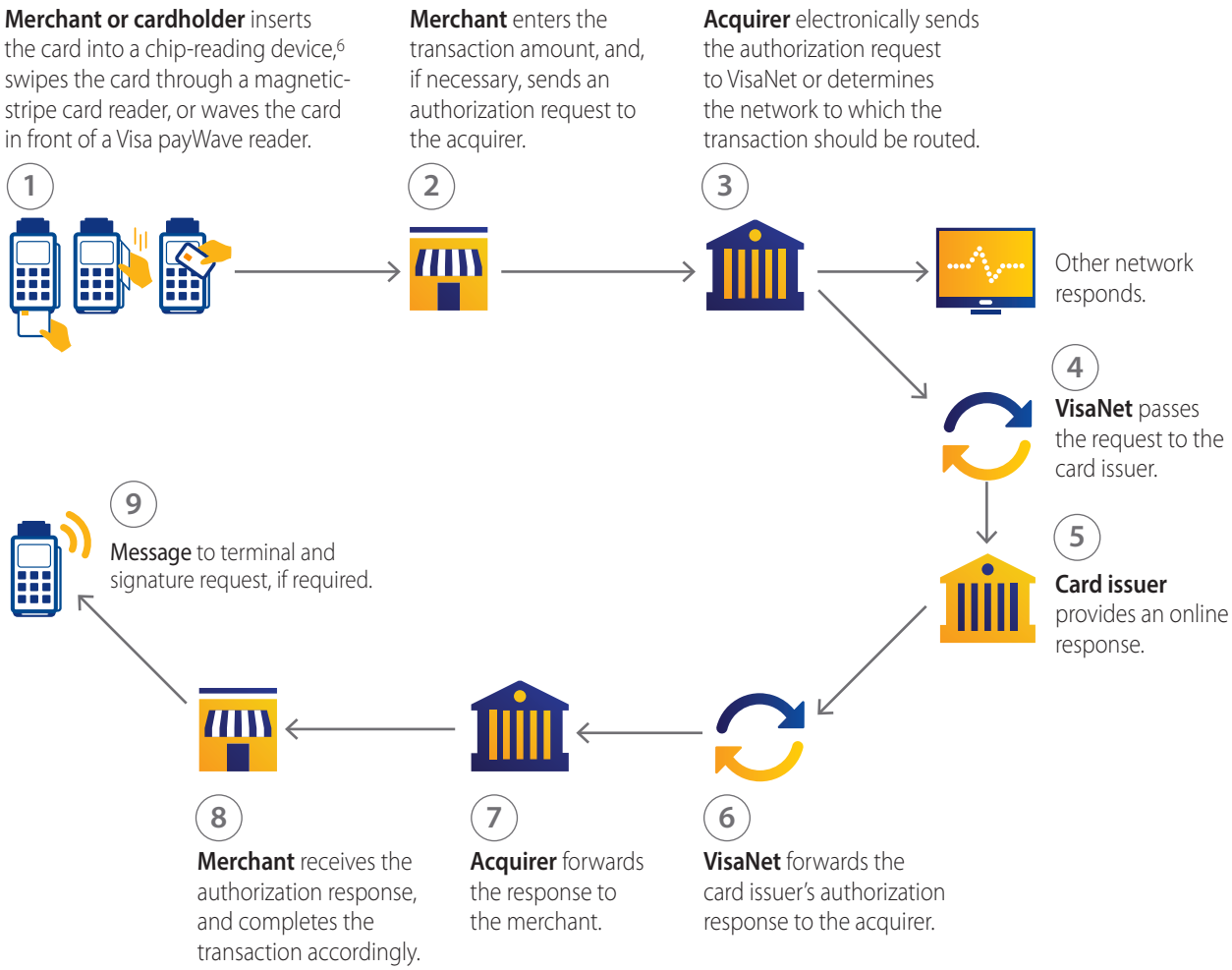
Transaction Flow in the Card-Present Environment

Transaction Life Cycles

The following illustrations show the life cycle of Visa card transactions in the card-present environment. 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.

CREDIT OR DEBIT TRANSACTION AUTHORIZATION PROCESS

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



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

[6] Many Visa cards are embedded with a chip. When used at a chip enabled POS terminal, the terminal will automatically prompt for the chip card to be 'dipped', instead of 'swiped' using the magnetic stripe.

TRANSACTION CLEARING AND SETTLEMENT PROCESS

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 final transaction (sometimes referred to as the "capture batch") to the acquirer.

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.

Chip Implementation

Introduction

The Chip Implementation section covers terminal configuration, testing, and AID requirements. All other specific chip best practices and procedures are detailed as they relate to the other sections in this guide.

The table below outlines the differences and similarities between chip and magnetic-stripe Visa transactions.

CHIP VS. MAGNETIC-STRIPE TRANSACTIONS

Characteristics of a Transaction	Similarities and Differences between Chip and Magnetic-Stripe Transactions
Transaction Requirements	**Similarity:** Requirements for payment with chip remain the same as with magnetic-stripe transactions. **Difference:** Procedures differ. • Chip cards are inserted ("dipped") into the reader and must remain inserted until the transaction is completed. Early removal of the card from the reader will terminate the transaction. • As terminal messages vary, any message that signals when a transaction is completed should be clearly identified. Merchants and their customers should be educated to remove the card from the terminal only after seeing this message. • Merchant staff should prompt cardholders to insert the card into the chip reader rather than swiping the magnetic stripe. This will make the transaction process faster and mitigate the potential problem where an issuer may have incorrectly personalized the card with a service code that does not correspond to the chip card.
Prepaid product features	**Similarity:** All prepaid features and functions such as activation discounts and loyalty programs will remain the same in chip card acceptance. **Difference:** None.
Point-to-point encryption	**Similarity:** Point-to-point should not impact EMV implementation, and vice versa, assuming that point-to-point encryption occurs outside of the EMV kernel which it always should. **Note:** There are many solutions available that can also go beyond the processor level to the network, as well. **Difference:** None.

Terminal Configuration

Given that the U.S. is a zero floor limit market and online infrastructure, Visa recommends supporting the U.S. Minimum Terminal Configuration Guidelines—see https://www.visa.com/chip/personal/security/chip-technology/index.jsp. The majority of U.S. chip cards will not support offline approvals.

These guidelines provide 100% protection against liability shift while significantly reducing implementation cost and complexity, and there are no requirements for offline functionality.

Contact and Contactless Chip Terminal Testing

Terminals must be tested prior to initial deployment to help ensure they are fully operational and configured correctly. Merchants should consult with their acquirer for their testing requirements.

Testing Toolkits

Visa developed the Acquirer Device Validation Toolkit (ADVT) and Contactless Device Evaluation Toolkit (CDET) to provide separate sets of test cards and test cases to be used on contact and contactless chip POS terminals prior to deployment.

These test cards help to ensure correct terminal configuration, assist with integration testing and meeting Visa's terminal requirements for both EMV contact chip and contactless chip devices.

The test results for ADVT and CDET, as appropriate, are submitted to Visa via the Chip Compliance Reporting Tool (CCRT).

Use of the ADVT and the CDET is intended to:

- Ensure basic contact and contactless chip functionality is not compromised during application integration.
- Ensure all Visa requirements are satisfied.
- Identify common interoperability issues.

Use of the toolkits does not imply or guarantee that a terminal is fully compliant with EMV specifications or Visa requirements.

The ADVT and the CDET can be obtained through Visa's third-party fulfillment service, Merrill Corporation. Similar tools are also available from Visa-confirmed third-party vendors.

Additional Support

For support materials and a list of Visa-confirmed tool vendors, see "Product Toolkits" at https://technologypartner.Visa.com.

These tools can help reduce required testing, standardize point-of-sale solutions, and modularize and/or isolate EMV chip functionality with the payment application.

More information about chip can be found at https://www.visa.com/chip/personal/security/chip-technology/index.jsp.

Visa Electron and Interlink AID Support

Visa Electron is issued exclusively outside the U.S.; Visa Electron transactions are processed as Visa transactions in the U.S., so Visa Electron can be accepted anywhere Visa is accepted. Interlink transactions can be accepted only at terminals capable of processing online PIN verification.

Merchants should continue to accept Visa Electron the same way they accept magnetic-stripe transactions today.

All chip-reading devices (contact and contactless) must contain the appropriate Application Identifier (AID). POS terminals and ATM devices must support the Visa Electron and Interlink (if applicable) AIDs to avoid interoperability issues:

- For Electron acceptance, the Visa Electron AID—A0000000032010—must be present. The Electron card itself will not contain the AID.
- For Interlink acceptance, the Interlink AID—A0000000033010—must be present.

If the required AIDs are missing from chip-enabled terminals, transactions from chip cards may be processed as fallback transactions.

Support for the Visa U.S. Common Debit AID is optional.

A table outlining the complete AID list for each product is included in the *Visa Minimum U.S. Online Only Terminal Configuration Guide* at https://usa.visa.com.

Fallback Procedures

When the Terminal Cannot Read the Chip

If the chip-reading device cannot read the chip on the card, the terminal should first fall back to magnetic stripe. Only if the magnetic stripe cannot be read should key-entry take place: key-entered transactions should always be the last option. Effective April 2017, key-entry acceptance is optional for EMV chip-enabled merchants.

Merchants should not force a fallback to magnetic stripe or key-entry, as they are more likely to see higher levels of authorization declines for these transactions from issuers than for valid chip transactions.

Visa strongly recommends that all card-present transactions be initiated with an electronic read, as opposed to key-entered. Electronically read data provides valuable risk management information to the issuer and appropriate protection to the merchant.

Major Causes of Fallback

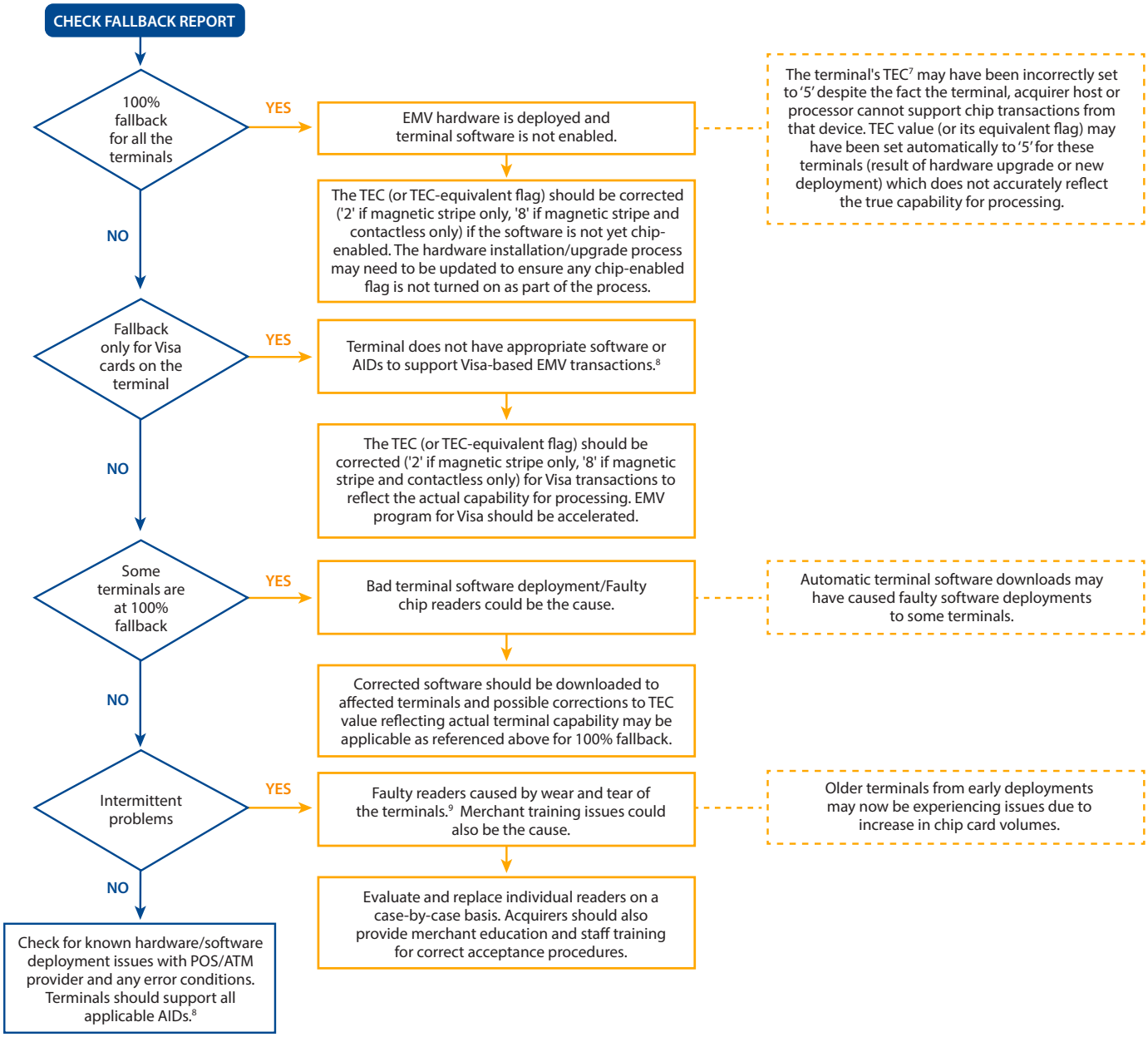
There are a number of reasons for fallback, ranging from data quality issues to faulty devices. It is essential that monitoring procedures be followed to ensure fallback levels are kept to a minimum.

The following flowchart outlines the major causes of fallback and the suggested recommendations to minimize it. The best way to minimize fallback is to analyze and monitor fallback reporting, checking for potential issues based on trends identified.

KEY POINTS TO REMEMBER

- ✔ 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-entry rules, as the counterfeit liability remains with the party that has not invested in chip technology.

FALLBACK RESOLUTION FLOWCHART



[7] TEC (Terminal Entry Capability) is a one-digit value that identifies a terminal's ability to electronically read account data from Visa cards or mobile devices. Value of 2 indicates the terminal can read only magnetic-stripe cards, 5 indicates the terminal can read contact chip cards and possible contactless chip form factors/mobile device or magnetic-stripe cards.

[8] Terminals must support the applicable AIDs to minimize fallback transactions. All POS terminals must support Visa AID and Visa Electron AID; ATM terminals must support Visa AID, Visa Electron AID, and Plus AID. To support Interlink acceptance, terminals must have the Interlink AID; and support for US Common Debit AID is optional.

[9] In some cases for ATMs, the chip reader might be inaccessible to the card due to damaged clamps, caused by wear and tear (clamps are used to hold the card). This could lead to fallback at these locations.

When a Card Won't Read When Swiped

A transaction is manually keyed into a point-of-sale (POS) device when a magnetic stripe cannot be read; key-entry procedures may be used at the POS as a last resort and only if fallback to magnetic stripe is not possible.

NOTE: Key-entry as a fallback is:

- **Required** if the merchant terminal is not chip-enabled.
- **Optional** if the merchant terminal is chip-enabled.

Key-entered transactions have different rules than chip fallback to magnetic stripe and should not be considered "fallback to magnetic stripe."

During the migration to chip, clients should ensure that staff are trained to follow the prompts on the terminal to avoid higher levels of key-entered transactions.

Counterfeit fraud chip liability shift also affects key-entered transactions. The liability remains with the party that has not invested in chip technology.

Key-Entered or Voice-Authorized Transactions

Key-entered[10] transactions should be processed by either:

- Making an imprint of the front of the card. The imprint proves the card was present at the POS and can protect a merchant's business from potential chargebacks if the transaction is 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.

  OR

- Including the Card Verification Value 2 (CVV2) in the authorization request for U.S. domestic key-entered transactions, in lieu of taking a manual card imprint (expires April 14, 2018).

Voice-authorized transactions must be processed with an imprint of the front of the card.

To minimize key-entered transactions, acquirers and merchants should implement staff training and monitoring to effectively pinpoint areas with high key-entry rates. The following monitoring steps help identify problem areas:

- Calculate the percentage of key-entered transactions compared to total transactions to pinpoint which stores, terminals, or sales associates have high key-entry rates.
- Monitor key-entry fallback rates on a monthly basis, as these transactions are less secure and have higher processing fees.

Key-entered and voice-authorized transactions are not supported for Visa Electron cards or Unattended Cardholder Activated Terminals (UCATs).

For key-entered transactions, an issuer chargeback for Reason Code 81—Fraud – Card Present is valid unless:

- The merchant can provide an imprint for domestic and international transactions.
- The merchant captured the CVV2 for U.S. domestic transactions only (expires April 14, 2018).

Deferred or Delayed Authorizations

Deferred or delayed authorizations may occur when the device does not have online capability and the online authorization is performed after the card is no longer available. Merchants performing this type of authorization should complete it within 24 hours of the transaction. When authorization processing is back online, the merchant should request an authorization and only submit approved transactions for clearing and settlement.

Because the U.S. has a zero floor limit, a merchant who supports the completion of transactions when authorization systems are offline will have several other considerations and requirements.

Prior to submitting transactions for settlement, acquirers or merchants who do not obtain online approval do so at their own liability. Also, it is important to note that this practice is against Visa Rules. Consult your acquirer for more information.

Properly Place Contactless Readers

Properly place contactless readers to ensure seamless usage by cardholders and maintain the principle of a fast transaction. Best practices include:

- Ensuring the reader is free from obstructions and easily accessible for cardholders to use the contactless payment feature.
- Placing contactless card readers at least 12 inches away from each other. In retail locations where the counter space is limited, the magnetic field of multiple readers in close proximity may overlap. This can disrupt the contactless transaction when a single contactless card is presented.
- Displaying the contactless symbol on all readers to let cardholders know "how and where" they can use Visa payWave cards.

Support of No Cardholder Verification Method and PIN

PIN pads remain a requirement for POS terminals that process debit transactions via Interlink.

It is recommended when accepting online PIN for magnetic-stripe debit, to also accept chip debit with online PIN.

It is not required that offline PIN be supported when supporting online PIN, as those offline PIN-preferring cards from foreign markets are also required to support signature, allowing for traditional acceptance in the U.S. market.

Finally, if a merchant does not support PIN today, there is no Visa requirement to support PIN with chip in any format.

If participating in VEPS, terminal capabilities will need to be programmed on installation based on transaction parameters.

All online-capable chip-enabled (contact and contactless) terminals must support the processing of transactions without a CVM.

Visa Rules for PIN-less Payment Brand Acceptance

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

Three Important Steps

1. Offer the Customer a Clear Payment Choice

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

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

2. Honor the Choice

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

3. Confirm the Choice

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

- Terminal branding (including new rules on contactless branding) see Point-of-Sale Branding flyers
- Requirements and Best Practices

Visa Branding of Payment Terminals

Visa has developed a set of guidelines and artwork to be used by acquirers, merchants, and other partners to accurately reproduce the Visa brand mark and the contactless symbol on payment terminals, as outlined briefly below. The complete guidelines and artwork are available from Visa. To obtain a copy, contact your acquirer.

Visa Point-of-Sale Graphic (POS)

- The Visa Point-of-Sale (POS) Graphic is for use where Visa payment products are accepted.
- All physical merchant locations, online merchant locations, and ATMs that accept Visa products for payment or cash disbursement must display the Visa POS Graphic. When using the Visa POS Graphic with other network marks we recommend placing Visa in the first position.
- In countries where use of Visa payWave is required, the Visa payWave POS Graphic would be used in addition to the Visa POS Graphic.
- The Visa POS Graphic should not be used in place of the Visa Brand Mark in any applications including on cards, in co-brand marketing materials or sponsorship lockups.

Display the Visa POS Graphic where Visa is accepted.

Visa POS Graphic with payWave where payWave is accepted.

The Contactless Symbol

- The Contactless Indicator is used on payment devices to indicate contactless payment technology. It is required on all terminals that meet ISO 14443 and EMVCo Contactless specifications.

Visa Easy Payment Service (VEPS)

Visa Easy Payment Service (VEPS) is a global program that allows qualifying low-value transactions of $25 or less at specific merchants to take place without cardholder verification. A receipt is not required unless requested by the cardholder. Quick Service Restaurants (MCC 5814) are eligible to participate in VEPS for in-store transactions.

Use VEPS to make payment processing faster and easier for both merchants and customers while increasing sales. This is especially beneficial to high-volume merchants since it allows merchants to serve more customers and reduces customer time spent in line.

As part of the VEPS program, merchants:

- Do not need to register for VEPS. If you are eligible to participate, contact your merchant bank or processor.
- Are not obliged to respond to issuer requests for copy for eligible transactions—meaning merchants do not need to store receipts for VEPS-qualified transactions.
- Are protected from illegible fulfillment (transaction receipt) such as: Transaction not recognized and Fraud – Card-Present chargebacks.

PIN Security

Visa is committed to protecting Visa cardholder PIN data. To that end, Visa created a PIN Security Program outlining compliance requirements. Acquirers, their merchants and/or their third-party agents must comply with this program.

The baseline requirements for the Visa PIN Security Program include:

- *Payment Card Industry (PCI) PIN Security Requirements*
- *Visa PIN Security Program Guide*

When purchasing PIN entry devices ensure you check they are on the *Approved PIN Transaction Security (PTS) Devices* list.

In addition to the PED requirements, Visa maintains a list of compromised PEDs.

- Visa Triple Data Encryption Standard (TDES) Requirements are:
  - All ATMs must use TDES to protect pins
  - All POS PIN acceptance devices must use TDES to protect pins. AFDs must use TDES or SDES DUKPT to protect pins.

Adherence to the requirements of the Visa PIN Security Program results in more than simply securing PIN data. Sound security practices help to protect organizations from adverse financial and reputational consequences often associated with PIN data compromises.

Merchants that acquire PIN transactions and/or perform key-management services for only their own acquiring business must perform appropriate due diligence to ensure compliance with the PIN Security Program requirements. This may include performing self-assessments using an internal or external resource. Individuals performing the self-assessment must have adequate knowledge of the PCI PIN Security requirements but do not need to be Visa approved PIN Security Assessors.

Self-assessment results do not need to be submitted to Visa; however, Visa may request evidence of PIN security compliance or request an on-site PIN Security review of any organization, at any time, to ensure the security of the payment system. A PIN Self-Assessment Questionnaire (PIN SAQ) template is available on Visa's PIN Security website, www.visa.com/pinsecurity.

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.pcisecuritystandards.org** for guidelines on these technologies.
More information about the PCI DSS, including Visa validation requirements and a suite of security tools and resources to support compliance, is available at **www.Visa.com/CISP**.
A listing of PCI approved PEDs can be found at **www.pcisecuritystandards.org**.

Fraud Mitigation

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 following chart summarizes the most common reasons for high key-entry rates and provides possible solutions.

POSSIBLE KEY-ENTRY CAUSES AND 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, dip, 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.

VISA BRAND MARK CARD SECURITY FEATURES

What to Look For On All Visa Cards

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.

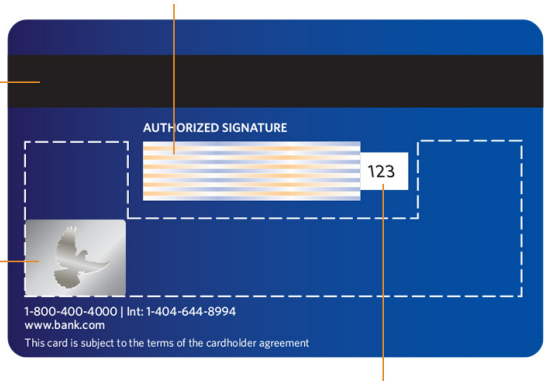
Ultraviolet V is visible over the Visa logo when the card is placed under an ultraviolet light.

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.

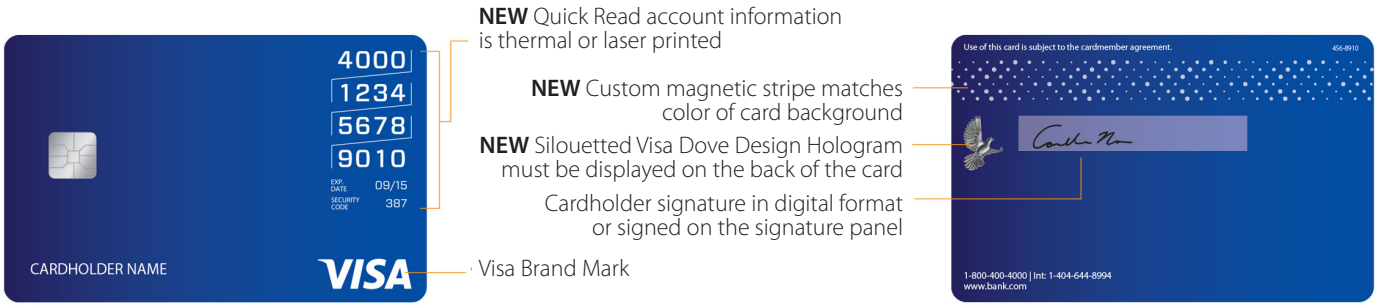
Card Verification Value 2 (CVV2)[11] is a unique three-digit code next to the signature panel of all valid cards.

[11] 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, dip, 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; rather the merchant should ask for another form of payment.

UNEMBOSSED VISA CARD SECURITY FEATURES



OTHER VERSIONS OF VISA CARDS

VISA MINI CARD

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

VISA VERTICAL

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.

Chargeback Mitigation

A "chargeback" provides an issuer with a way to disupte a transaction. When a cardholder disputes a transaction, the issuer may request a written explanation of the problem from the cardholder and can also request a copy of the related sales transaction receipt from the acquirer, if needed. Once the issuer receives this documentation, the first step is to determine whether a chargeback situation exists. There are many reasons for chargebacks; for complete details review the *Chargeback Management Guidelines for Visa Merchants*. For the purposes of this document, we will concern ourselves with two fraud-related chargebacks that occur in card-present environments.

Reason Code 62: Counterfeit Transaction

Applied When:

The card issuer receives a complaint from the cardholder claiming he or she did not authorize or participate in the transaction.

Most Common Causes

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

- Failed to compare the first four digits of the embossed account number on the card with the preprinted digits below the embossed number for a card-present transaction.
- Received authorization without transmission of required data.

Merchant Actions – Administrative

- **Card and Transaction Were Valid**
  If the card was swiped and transaction was authorized at the point of sale, provide your acquirer with a copy of the printed sales receipt.
- **Transaction Was Counterfeit**
  If the transaction was counterfeit, accept the chargeback.

Merchant Actions – Preventive

- Deploy chip-enabled point-of-sale devices.

Reason Code 81: Fraud—Card-Present Environment

Applied When:

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

- The card issuer received a sales receipt that has no imprint of the card's embossed or magnetic-stripe information or the cardholder's signature, and either: the cardholder certifies that he or she neither authorized nor participated in the transaction OR the card issuer certifies that no valid card with that account number existed on the transaction date.
- A card-present transaction charged to a fictitious account number for which authorization approval was not obtained. This chargeback is not valid for recurring payments and card-absent transactions. It is valid for card-present sales on self-serve point-of-sale terminals such as unattended kiosks.

Most Common Causes

The merchant or service establishment:

- Did not swipe the card through a magnetic-stripe reader.
- Did not make a manual imprint of the card account information on the sales receipt for a key-entered transaction.
- Completed a card-present transaction without obtaining the cardholder's signature on the sales receipt.
- Completed a card-absent transaction, but did not identify the transaction as a MO/TO or Internet purchase.
- Accepted a chip card[12] containing a Visa or Visa Electron Smart Payment Application or an EMV and VIS-Compliant Plus application, but processed the chip card as a fallback transaction—via magnetic stripe, key entry or paper voucher, and did not follow correct acceptance procedures.

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

Merchant Actions

Train sales staff to:

1. Always electronically read (dip or swipe) every transaction,
2. Compare the signature on the receipt to the signature on the back of the card (the names must be spelled the same), AND
3. Accept only signed cards.

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

Custom Payment Service Qualification

The Visa Custom Payment Service (CPS) program outlines transaction data criteria and processing standards that U.S. merchants must meet to qualify for a CPS program—requirements that not only allow cost savings but may also help protect merchants against certain authorization-related and fraud-related disputes.

Attended Transactions

In a CPS/Restaurant transaction—the best qualification for a card-present transaction where the card was electronically read—the card, cardholder, merchant, and terminal are all present. The magnetic stripe or chip is read, the authorization request is approved, the receipt is typically signed, and the cardholder's signature is typically verified.

To qualify for the CPS/Restaurant program, a transaction must have the following characteristics:

- One authorization per clearing transaction is allowed.
- The card must be present at the point of sale.
- Complete and unaltered contents of Track 1 or Track 2 of the card's magnetic stripe must be read and transmitted, or unaltered chip data must be sent.
- MCC must be 5812 (Restaurant) or 5814 (Fast Food).
- Transaction must clear in two days.
- Purchase date must be within one day of the authorization date.
- Cardholder's signature must be obtained, unless the transaction qualifies as a
- Visa Easy Payment Service (VEPS) Transaction.
- If a debit card transaction, it must also have the merchant name and location included in the authorization request.

CPS Key Entry Program Qualification

In a CPS/Retail Key Entry transaction (the best qualification for a card-present transaction where the card was not electronically read), the card, cardholder, merchant, and terminal are all present. The magnetic stripe cannot be read, the authorization request is approved, the receipt is signed, and the cardholder's signature is verified.

To qualify for the CPS/Retail Key Entry (Credit or Debit) program, a transaction must have the following characteristics:

- One authorization per clearing record allowed.
- Cardholder must be present and signature must be obtained.
- Card must be present, with key entry due to failure in reading the magnetic stripe.
- Must not be a mail order/telephone order (MOTO) or ecommerce transaction.
- Transaction must clear in two days.
- Address Verification Service (AVS) is requested in the authorization, resulting in a ZIP Code match, retry, or unsupported AVS result.
- Purchase date must be within one day of the authorization date.

Unattended Transactions

In a CPS/Small Ticket transaction, the cardholder and card are present at the merchant location. The magnetic stripe or chip is read, and the authorization request is approved. Signature is not required, and a receipt is required only upon cardholder request.

To qualify for the CPS/Small Ticket (Credit or Debit) program, a transaction must have the following characteristics:

- One authorization per clearing transaction is allowed.
- The card must be present at the point of sale.
- Cardholder and card must be present at the merchant location.
- Merchant or merchant's representative may not be present.
- Complete and unaltered contents of Track 1 or Track 2 of the card's magnetic stripe must be read and transmitted, or unaltered chip data must be sent.
- Transaction must be from a U.S. merchant.
- Merchant name and location must be included in the authorization and in the clearing record.
- Transaction must clear in two days.
- Transaction is not from an ineligible MCC.
- Transaction amount must be less than or equal to $15.00.
- Cardholder signature is not required.
- Purchase date must be within one day of the authorization date.

Section 2. Visa Acceptance in the Card-Absent Environment

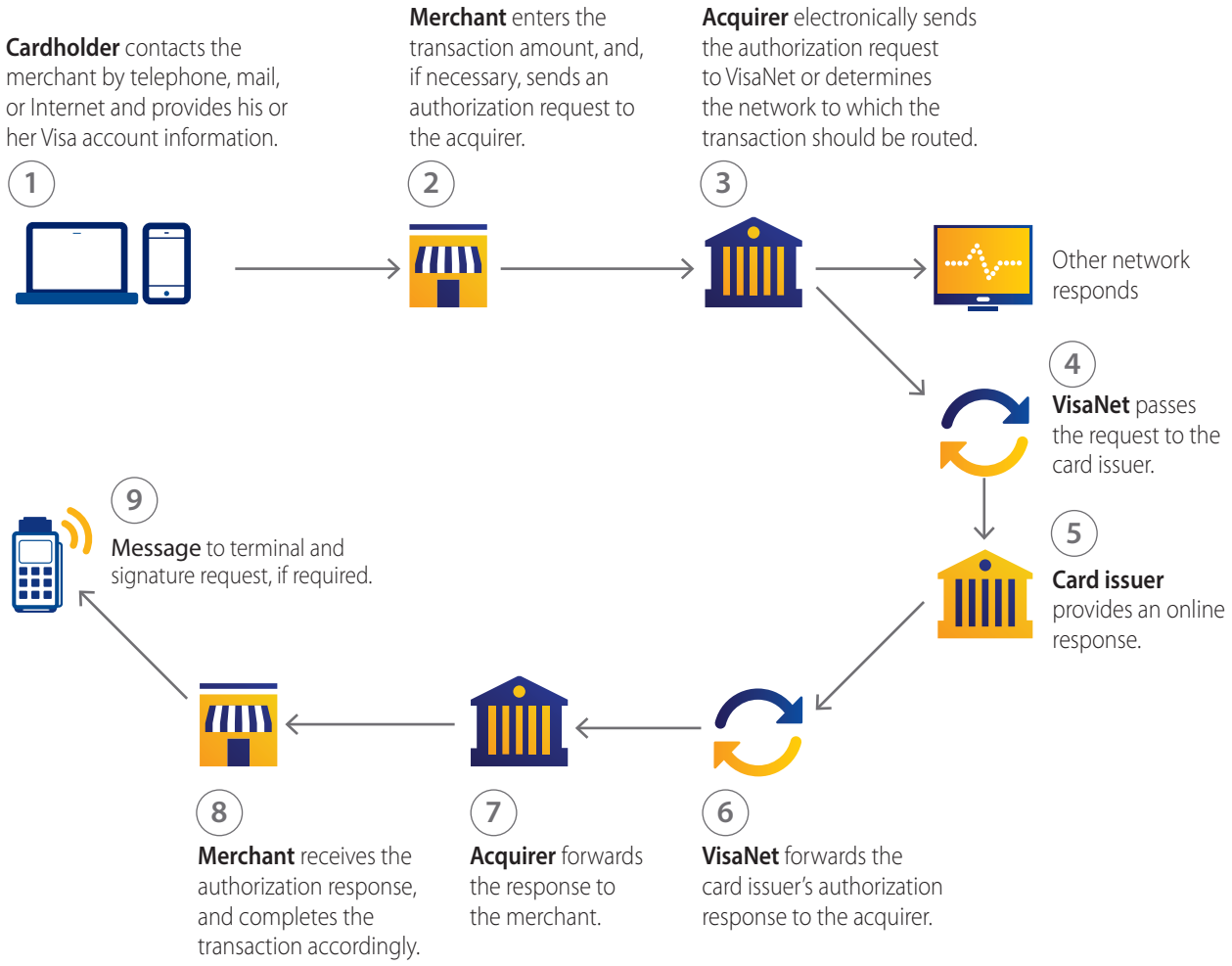
The growth of the ecommerce, mail order/telephone order (MO/TO), and mobile app merchant channels means increasing numbers of QSR merchants are now processing transactions in situations where the card and cardholder are not present—and fraud may be especially difficult to detect. Of necessity, card acceptance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

Visa Transaction Flow for Card-Absent Transactions

Transaction Life Cycles

The following illustrations show the life cycle of Visa card transactions for both 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.

CARD-ABSENT CREDIT OR DEBIT TRANSACTION PROCESS



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

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

TRANSACTION CLEARING AND SETTLEMENT PROCESS

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 acquirer.

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.

Card-Absent Transaction Processing Best Practices

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)[13], Address Verification Service (AVS)[14], and Verified by Visa.
- Perform internal screening (e.g., velocity checks, negative database, etc.) or use third-party tools to screen for questionable transaction data or other potential warning signs indicating "out of pattern" orders. Route transactions with higher risk characteristics for fraud review.

[13] In certain markets, CVV2 is required to be present for all card-absent transactions.
[14] AVS is only available for U.S. and Canadian issued cards

Custom Payment Service Qualification

The Visa Custom Payment Service (CPS) program outlines transaction data criteria and processing standards that U.S. merchants must meet to qualify for a CPS program—requirements that not only allow cost savings but may also help protect merchants against certain authorization-related and fraud-related disputes.

Three programs that apply to the card-absent environment are discussed here:

- Mail order/telephone order transactions
- Electronic Commerce Preferred
- Electronic Commerce Basic

Mail Order/Telephone Order Transactions

In a Custom Payment Service (CNP) card-not-present transaction, the card and the cardholder are not at the merchant location. The magnetic stripe or chip cannot be read, the authorization request is approved, the receipt is not signed, and the cardholder's address may need to be verified.

Characteristics Required

To qualify for the CPS/Card-not-Present (Credit or Debit) program, a transaction must have the following characteristics:

- Merchant accepts payment by mail or telephone. (Electronic commerce transactions do not qualify for this program. See the following pages.)
- Card and cardholder are not at the merchant location.
- POS terminal application is equipped to provide additional data such as the merchant.
- order number and customer service telephone numbers.
- One or more clearing record message per transaction is allowed.
    - One reversal is permitted to make total authorization amount equal to clearing amount.
- In most cases, address verification request is required in authorization.
- Transaction must clear in two days and include:
    - Purchase date, which is the ship date,
        - Within seven days after the authorization date (or one day prior to the authorization date)
    - Customer service telephone number, Uniform Resource Locator (URL), or email address (as applicable),
    - Order number,
    - Mail/Phone/Electronic Commerce and Payment Indicator (ECI), and
    - Total Authorized Amount.
- Multiple clearing messages are identified by the ticket sequence number and count.

Electronic Commerce Preferred—Retail (Credit or Debit) Program Qualification

In a CPS/Electronic Commerce Preferred—Retail transaction, the card and the cardholder are not at the merchant location and the transaction takes place in a secure Internet environment utilizing Verified by Visa. The magnetic stripe cannot be read or the chip is not required to be read, the authorization request is approved, and the receipt is not signed.

To qualify for the CPS/ Electronic Commerce Preferred—Retail (Credit or Debit) program, a transaction must have the following characteristics:

- Identified as a secure ecommerce transaction utilizing the CAVV Verification Service
    - An "Authenticated" transaction occurs when the merchant, acquirer, issuer, and cardholder all participate in Verified by Visa and the issuer provides an "Authentication Confirmation" to the merchant.
    - An "Attempt" transaction occurs when the merchant and the acquirer participate in Verified by Visa and the merchant receives an "Attempt Response" from the issuer or Visa on the issuer's behalf.
- Card and cardholder are not at the merchant location.
- Must have valid 3-D Secure fields present in the authorization:
    - CAVV
    - MOTO/ECPI
- POS terminal application is equipped to provide additional data such as the merchant order number and customer service telephone numbers.
- One or more clearing record message per transaction is allowed.
    - One reversal is permitted to make total authorization amount equal to clearing amount.
- Address verification request is required in the authorization, except for transactions from select developing m market MCCs and transactions from MCC 4900.
- Transaction must clear in two days and include:
    - Purchase date, which is the ship date (up to 7 days from authorization),
        - For mail/phone order or electronic commerce transactions, the ship date is the transaction date.
    - Customer service telephone number, URL or email address (as applicable), Order number,
    - MOTO/ECPI, and
    - Total authorized amount.

CPS/Electronic Commerce—Basic (Credit or Debit) Program Qualification

The CPS/Electronic Commerce—Basic (Credit or Debit) program applies to retail merchants that process ecommerce transactions. The card and the cardholder are not at the merchant location and the transaction takes place in a secure Internet environment. The magnetic stripe cannot be read or the chip is not required to be read, the authorization request is approved, the receipt is not signed, and AVS may not be required. The transaction is not required to utilize Verified by Visa. This program is available if the Verified by Visa service was utilized, but the transaction cannot qualify for CPS/Electronic Commerce Preferred—Retail due to an invalid card type, transaction type, or CAVV data.

To qualify for the CPS/Electronic Commerce—Basic (Credit or Debit) program a transaction must have the following characteristics:

- Identified as an ecommerce transaction processed in a secure environment. Card and cardholder are not at the merchant location.
- POS terminal application is equipped to provide additional data such as the merchant order number and customer service telephone numbers.
- One or more clearing record message per transaction is allowed.
- One reversal is permitted to make total authorization amount equal to clearing amount.
- Address verification request is required in authorization, except for select developing market transactions and transactions from MCC 4900.
- Transaction must clear in two days and include:
    - Purchase date, which is the ship date (up to 7 days from authorization),
        - For mail/phone order or electronic commerce transactions the ship date is the transaction date.
    - Customer service telephone number, URL or email address (as applicable),
    - Order number,
    - MOTO/ECPI, and
    - Total authorized amount.

Fraud-Prevention Guidelines for Card-Absent Transactions

Authorize All 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.

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.

Fraud-prevention guidelines and best practices for card-absent merchants

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

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 counterfeit or other unauthorized use.

Ask for CVV2

The Card Verification Value 2 (CVV2)[15] is a three-digit security number printed on the back of Visa cards to help validate that a customer is in possession of the card at the time of an order. *(See Visa Card Features and Security Elements on page 26.)*

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 too.

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

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[16] presence indicators, even if you are not including a CVV2 in your authorization request:

PRESENCE INDICATORS

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 CODES

Result:	Action:
M – Match	Complete the transaction (taking into account all transaction characteristics and any questionable data).
N – No Match[17]	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.

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.

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

[17] 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

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:

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

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

AVS Processing Options

AVS Processed as Part of an Authorization Request

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

AVS Processed As Part of Account Verification Request

A merchant may also send an AVS request without an accompanying authorization request by using the Zero Amount Account Number Verification Service[18], which is available in all regions. For example:

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

How to Use AVS

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

- When a customer contacts you to place an order,
  - Confirm the usual order information.
  - Ask the customer for the billing address (street address and/or ZIP or postal code) for the card being used (i.e., the billing address is where the customer's monthly Visa statement is sent for the card being used).
  - Enter the billing address and the transaction information into the authorization request system and process both requests at the same time.
- The card issuer will make an authorization decision separately from the AVS request and compare the cardholder billing address sent with the billing address for that account. The card issuer will then return both the authorization response and a single character alphabetic code result that indicates whether the address given by the cardholder matches the address on file with the card issuer.

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

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

Address Verification Results 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."

Code	Definition	Code Applies To: Domestic	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

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
Y	**DFM**	**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 in its file or have the same address information in a different format; the cardholder may have recently moved; merchant staff may have entered the address incorrectly; or this response may indicate a potentially fraudulent situation.
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 explanations provided here are meant to give you enough information to make your own determination of what works best for you.

One merchant may treat these codes differently than the way another merchant treats the same codes.

International Addresses

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

ZIP, POSTAL CODE-ONLY, AND PO BOX ADDRESSES

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 –SIP Code/Postal Code Matches).

Additional Fraud-Prevention Tools for the Internet

Verified by Visa

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 provides merchants with cardholder authentication on ecommerce transactions. Verified by Visa helps reduce ecommerce fraud by helping to ensure that the rightful owner of the Visa account is initiating the transaction. 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[19] mismatch or CVV2[20] 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 .

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

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

CyberSource[21]

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[22] 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.

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**.

21 CyberSource is a wholly owned subsidiary of Visa.

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

Ethoca Alert Technology

- 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 affected 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@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.

Mail Order/Telephone Order Customer Behavior

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

- **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.

Ecommerce Customer Behavior

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 a criminal's profits.

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.

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.

Transaction Characteristics

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.

Website Guidelines

Today, more and more merchants are adding online sales to their traditional card-present operations. As a result, Visa has developed guidelines 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.
- Delivery policy. Merchants set their own policies about delivery of goods—that is, if they have any geographic or other restrictions on where or under what circumstances they provide delivery. Any restrictions on delivery must be clearly stated on the website.
- Country of origin. You must disclose the permanent address of your establishment on the website. Check with your acquirer to ensure your disclosure is made in accordance with the Visa Core 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 customers.
- 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.

Chargeback Mitigation for Card-Absent Merchants

A "chargeback" provides an issuer with a way to return a disputed transaction. When a cardholder disputes a transaction, the issuer may request a written explanation of the problem from the cardholder and can also request a copy of the related sales transaction receipt from the acquirer, if needed. Once the issuer receives this documentation, the first step is to determine whether a chargeback situation exists. There are many reasons for chargebacks; for complete details review the *Chargeback Management Guidelines for Visa Merchants*. For the purposes of this document, we will concern ourselves with fraud-related chargebacks that occur in card-present environments.

Reason Code 83: Fraud—Card-Absent Environment

When to Apply Reason Code 83

The card issuer received:

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

Card-absent transactions include mail order, telephone order, Internet, pre-authorized health care transactions, recurring and advance payment transactions, and no-show fees.

Note: The pre-authorized health care transaction provision only applies to U.S. transactions.

Most Common Causes

The merchant:

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

The cardholder:

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

Merchant Actions

Back-Office Staff: Possible Remedies

Authorization Was Obtained and AVS or CVV2 Used

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

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

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

Authorization Obtained, AVS or CVV2 Not Used

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

Card-Present Transaction

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

Recurring Payment

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

Point-of-Sale Staff: Preventive Measures

Obtain Authorization for All Card-Absent Transactions	Always request authorization for mail order, telephone order, Internet, and recurring transactions, regardless of the dollar amount.
Verify Account	For telephone transactions, always verify (read back) the account number with the customer to avoid errors.
Number with Customer Identify Transaction as Card-Absent	All card-absent transactions should be identified by the appropriate code for MO/TO or Internet during both the authorization and settlement process. In most cases, this will be done automatically by your transaction-processing terminal or system, or by pressing a MO/TO indicator button. If not, be sure to write the appropriate code on the transaction receipt: "MO" for mail order; "TO" for telephone order; and "ECI" for Internet.

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

Owner/Manager: Preventive Measures

Risk-Management Tools

For card-absent transactions, consider using AVS[23], CVV2[24], and Verified by Visa to help reduce fraud. Contact your acquirer for more information on these important risk-management tools.

Identifying Card-Absent Transactions

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

Merchant Name

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

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

.

[23] AVS is only available in the U.S. and Canada.

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

Section 3. Important Information for Both Card-Present and Card-Absent Environments

As one might expect, there are a number of aspects of Visa card acceptance that apply to both the card-present and card-absent environments. This section will include important information regarding the following:

- Special Authorization Processes
- Interchange Overview
- Cardholder Data Security
- Compelling Evidence in the Dispute-Resolution Process

Special Authorization Processes

Partial Authorization

Merchants are encouraged to participate in the Visa Partial Authorization service. Visa Partial Authorization enables participating merchants to receive an approval for a partial amount of a transaction—for example, the amount available on a prepaid card or in a debit card account balance—when the amount in the original authorization request exceeds the available card balance.

The issuer is able to return an authorization response with an approval for a portion of the original amount requested. This enables the transaction to be capped at the partial authorized amount. If the merchant wishes to dispense above the amount returned in the partial authorization response, the remainder of the transaction amount can be paid by other means using split-tender functionality, where applicable.

This service provides an alternative to receiving a decline when the available card balance is not sufficient to approve a transaction in full and can result in increased sales for the merchant.

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.

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**
  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**
  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**
  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.

Interchange Overview

Interchange and Pricing

Payment acceptance has associated costs that need to be closely monitored and managed. An important component of this cost is the Interchange Reimbursement Fee (IRF) paid by the merchant bank to the card issuer and often passed through to the merchant.

Interchange rates are determined based on the type of merchant, type of card product, and the manner in which the transaction is processed. If a transaction is not processed in accordance with rate qualification criteria, it may be downgraded to a more expensive interchange rate. In controlling card acceptance costs, it is imperative that quick-service merchants control interchange downgrades.

Interchange Best Practices

Interchange best practices include:

- Ensuring that the transaction qualifies for the appropriate Custom Payment Service (CPS) program.
- Using VEPS (Visa Easy Payment Service) for appropriate in-store transactions under $25.00.
- Avoiding downgrades that result from miscoded transaction files. Consider the following:
    - Carefully testing initial deployment and any subsequent changes to the POS system.
    - Ensuring that each POS is coded to the proper Merchant Category Code (MCC).
- Ensuring that transaction-clearing batches are transmitted to the merchant bank at least once a day.
- Working with the merchant bank to ensure correct interchange is assigned to all transactions. Merchant banks should be capable of providing the underlying volume by the rate category detail that is needed to monitor qualification levels.
- Using peer benchmarks and historical patterns to identify anomalies in qualification patterns in conjunction with the merchant bank.
- Conducting root-cause analysis in order to understand the causes of downgrades (such as failed PIN pads, breakdowns in telecommunications technology, misprogrammed POS software, etc.).

Avoiding Transaction Integrity Fees

To avoid Transaction Integrity Fees (TIF), acquirers and merchants need to ensure that U.S. domestic and interregional Visa Debit card and Visa Prepaid card purchase transactions request CPS participation and meet CPS qualification.

Cardholder Data Security

Introduction

The Cardholder Data Security section focuses on the tools and controls to safeguard cardholder data. It addresses how to deal with attacks by fraudsters through skimming devices. It also covers Payment Card Industry Data Security Standard (PCI DSS) compliance and the validation of compliance.

Payment Card Fraud Major Concern for Quick-Service Merchants

Payment card fraud can be a major concern for quick-service merchants. Unattended terminals are easy to access for the fraudster who wishes to remain anonymous.

The fraudster may wish to attack the terminal as a point of compromise, attempting to capture payment or PIN data, or as a means to check fraudulent cards.

Payment Card Skimming Devices

Fraudsters can target self-service terminals by installing skimmers to capture payment card data. It is important to understand the current threats and risks to properly safeguard against skimming devices.

Ensuring Point-of-Sale Device 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.
- 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, and in a manner consistent with access laws pertaining to the disabled.

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 **visa.com** or contact your acquirer.

What to do if Skimming Devices are Discovered

If skimming devices are discovered, take the following steps:

- Do not approach or confront anyone who looks suspicious, or who is installing or removing a skimming device.
- Document and take pictures of the skimming device.
- Use protective gloves to remove the device.
- Contact the local authorities and U.S. Secret Service.

PCI DSS Compliance

Most merchant banks work very closely with their retailers to define the appropriate types of tools and controls they need to actively manage payment system risk and limit related exposures.

The PCI Data Security Standard (PCI DSS) is a comprehensive set of international security requirements for protecting 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. PCI DSS compliance protects the merchant from being a point of compromise.

- The PCI DSS consists of twelve basic requirements. These requirements are the foundation of Visa's data security compliance program.
- All Visa acquirers and 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.

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.

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 12 basic requirements, which are supported by more detailed sub-requirements.

PCI DSS Basic Requirements	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 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. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Validation of Compliance

Separate from the mandate to comply with PCI DSS is the validation of compliance. Validation ensures the merchant has achieved PCI DSS compliance and helps ensure that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined validation levels based on volume of transactions and the potential risk and exposure introduced into the Visa system. All merchants are required to re-validate PCI DSS compliance annually.

The requirements found in the *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements* and *PCI PIN Security Requirements* documents are intended to protect Visa cardholder PINs both in the POS and in the transporting networks. Both documents can be found at **https://www.pcisecuritystandards.org/document_library**.

Visa requires both PCI PTS POI and PCI PIN compliance for all PIN entry. This compliance includes mandates to use Triple DES to protect PIN data. Once an authorization is sent, PIN data should be erased to eliminate any opportunity for subsequent exposure of PIN data.

Compelling Evidence in the Dispute-Resolution Process

In its ongoing efforts to better align and simplify processes and procedures, Visa has refined the dispute-resolution process for merchants by adding representment-processing requirements for compelling evidence. Compelling evidence allows merchants to provide additional types of evidence to try and prove the cardholder participated in the transaction, received the goods or services, or benefited from the transaction.

"**Compelling evidence**" is providing proof the cardholder participated in the transaction, received the goods or services, or benefited from the transaction.

Compelling Evidence Reason Codes

Merchants now have a representment right to provide compelling evidence for the following chargeback reason codes:

- Reason Code 30 Services Not Provided or Merchandise Not Received
- Reason Code 53 Not as Described or Defective Merchandise
- Reason Code 81 Fraud – Card-Present Environment
- Reason Code 83 Fraud – Card-Absent Environment

For merchants, it's important to remember that this is only a representment right and not a remedy for the chargeback.

Issuers Must Address Compelling Evidence

With compelling evidence representment rights for merchants comes the need to ensure issuers provide this information to their cardholders. If compelling evidence is provided by the acquirer with the representment, issuers must attempt to contact their cardholder with this new information. Issuers are required to provide certification through Visa Resolve Online that an attempt to contact the cardholder with the compelling evidence has been made.

Pre-Arbitration Requirement for Issuers

Prior to filing an arbitration case with Visa, if the issuer refutes the compelling evidence provided with the representment by the acquirer, the issuer must initiate a pre-arbitration case prior to filing arbitration with Visa. If the issuer files an arbitration case with Visa without initiating a pre-arbitration first, the issuer will receive an unfavorable arbitration ruling.