REDUCING COUNTERFEIT FRAUD THROUGH ACCEPTANCE BEST PRACTICES

Table of Contents

Introduction

Managing Counterfeit Fraud

It is typical after a data compromise to see attempts at conducting domestic and cross-border counterfeit fraud.

In response to this growing threat, Visa is continuing to move expeditiously to enhance payment card security and strengthen all efforts to combat counterfeit fraud. This document provides insights into counterfeit fraud prevention best practices and procedures. It is intended to help all U.S. acquirers and merchants reduce their exposure to counterfeit transactions and minimize fraud losses.

Key topics includes:

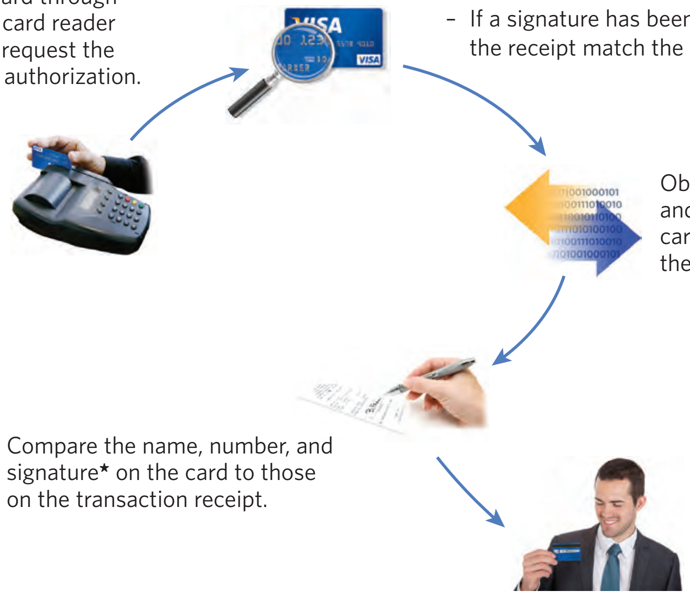
- Following proper card acceptance procedures
- Using Visa card security features to identify valid and suspicious cards
- Ensuring cardholder verification and identification
- Identifying suspicious behavior

Proper Card Acceptance Procedures

Whether sales associates are experienced or new to the job, if they follow a few basic card acceptance procedures, they will do it right the first time and every time.

The following illustrations provide an overview of the card acceptance steps that should be used at a point-of-sale terminal. Each step is explained in greater detail in this document.

Illustration of Card Acceptance (Magnetic Stripe Card Processing)



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

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

- Are the security features on the card valid?
- Do the first/last four digits embossed on the card match the first/last four digits on the magnetic stripe?
- If a signature has been obtained, does the signature on the receipt match the signature on the back of the card?

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

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

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

If card-present merchants follow proper card acceptance procedures at the point of sale, they will not be liable for fraud losses should they occur.

* The cardholder signature is not required if the transaction is PIN-verified, or processed with Visa Easy Pay Service (VEPS).

Visa Card Features and Security Elements

What to Look For On All Visa Cards

Visa Brand Mark Card Security Features

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.

Checking card features and security elements helps to ensure that the card is valid and has not been altered in any way.

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

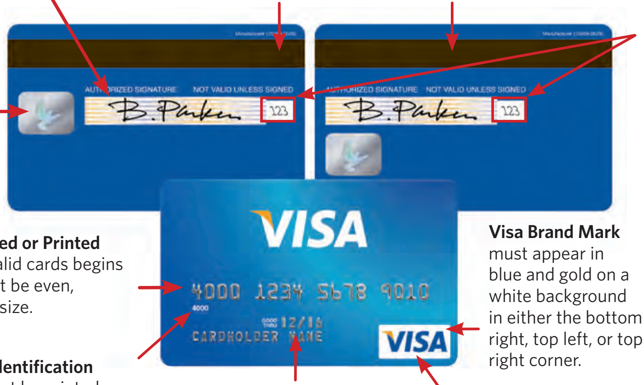
The words "Authorized Signature" and "Not Valid Unless Signed" must appear above, below, or beside the signature panel.

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

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

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

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)* is a three-digit code that appears either in a white box to the right of the signature panel, or directly on the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-not-present transactions to verify that customer is in possession of a valid Visa card at the time of the sale.

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

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

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

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

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

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

Chip cards contain a small embedded microchip that is virtually impossible to copy or counterfeit.

Chip Antenna for contactless cards, the interface can be an antenna embedded into the back of the card and connected to the chip.

A contactless transaction works at terminals through the radio frequency wave between the card and the terminal.

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.

* In certain markets, CVV2 is required to be present for all card-not-present 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.

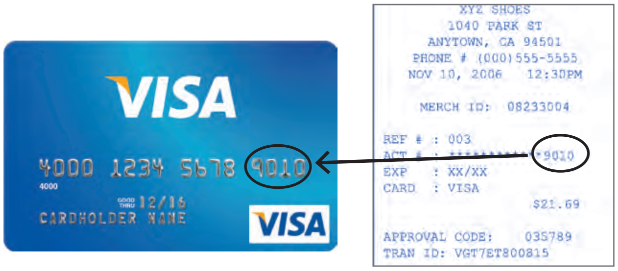
Cardholder Verification and Identification

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

Checking Signatures

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

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



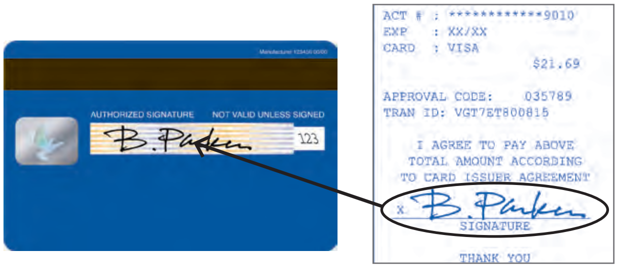
```
       XYZ SHOES
     1040 PARK ST
   ANYTOWN, CA 94501
 PHONE # (000)555-5555
 NOV 10, 2006   12:30PM

   MERCH ID:  08233004

REF #  : 003
ACT #  : ************9010
EXP    : XX/XX
CARD   : VISA
                   $21.69

APPROVAL CODE:    035789
TRAN ID: VGT7ET800815
```

- When a signature has been obtained, match the signature on the back of the card to the signature on the receipt. The first initial and spelling of the surname must match.



```
ACT #  : ************9010
EXP    : XX/XX
CARD   : VISA
                   $21.69

APPROVAL CODE:    035789
TRAN ID: VGT7ET800815

   I AGREE TO PAY ABOVE
  TOTAL AMOUNT ACCORDING
 TO CARD ISSUER AGREEMENT
X  B. Parker
       SIGNATURE

       THANK YOU
```

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

When a Signature Line is Not Present

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

Unsigned Cards

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

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

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

"See ID"

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

In this situation, follow recommended steps listed above under *Unsigned Cards*.

Requesting Cardholder ID

If a transaction is suspicious, you may ask the cardholder for an official ID to help mitigate fraud. However, it is important to remember that a Visa merchant must not require a cardholder to provide supplemental information such as government ID, driver's license, etc. as a condition of honoring the card.

If you are suspicious about the transaction or feel you need additional information to ensure the identity of the cardholder, adhere to your merchant store procedures and respond accordingly.

Terminal Unable to Read the Swipe

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

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

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

- Check the terminal to make sure that it is working properly and that you are swiping the card correctly.
- If the terminal is okay, take a look at the card's security features to make sure the card is not counterfeit or has not been altered in any way. (See *Visa Card Features and Security Elements* on page 3 of this document.)
- If the problem appears to be with the magnetic stripe, follow merchant store procedures. You may be allowed to use the terminal's manual override feature to key-enter transaction data for authorization, or you may need to make a call to your voice-authorization.
- For key-entered or voice-authorized transactions, make an imprint of the front of the card. The imprint proves the card was present at the point-of-sale and can protect your business from potential chargebacks if the transaction turns out to be fraudulent. The imprint can be made either on the sales receipt generated by the terminal or on a separate manual sales receipt form signed by the customer.
- If an unembossed card will not swipe, you should ask for another form of payment. Do not manually key enter unembossed cards unless you participate in the CVV2 with Magnetic-Stripe Failures process (see next page for details), or write the account number on a paper draft. A marked paper draft will not protect a merchant against chargebacks.

For some merchants, a high key entry rate is due to misclassification of card-not-present transactions so they look like card-present transactions. Consult with your acquirer to make sure your card-not-present transactions are correctly classified with accurate MO/TO and ECI indicators.

Use of CVV2 at the Point of Sale

Visa CVV2, which stands for Card Verification Value 2, and is also commonly known as the 3 digit code, is an important security feature on Visa cards. CVV2 is commonly used as a risk assessment tool by merchants who accept Visa cards for mail order/telephone order (MOTO) and online transactions. Although the intended use of CVV2 is in the card-not-present (CNP) channel, in some markets it has proven to be an effective tool in reducing fraud in the card-present environment where magnetic stripe data is used.

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

As CVV2 is not present on a magnetic stripe, it is not exposed through skimming or data sniffing and provides additional validation for an issuer in higher-risk transactions. In the card-present sales environment, CVV2 may be used for verifying that the card being used is a legitimate Visa card and not a counterfeit card. When a card-present merchant receives a CVV2 Result Code N – No Match, they have three options:

- Reject the transaction.
- Ask again for the CVV2 to obtain a match.
- Accept the transaction and the associated risk.

CVV2 validation should only be used for selective transactions that present higher risk to the merchant and issuer.

Merchants must not store CVV2 after authorization and must protect this data element in line with PCI DSS.

Suspicious Behavior

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

At the Point of Sale

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

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

If you feel uncomfortable or suspicious about a cardholder or transaction, adhere to your merchant store procedures and respond accordingly.

At Service Stations

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

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

Additional Resources

Documents and Publications

Materials for merchants that support U.S. domestic transactions are available at *www.visa.com/merchants*.

Visa offers a number of risk management materials as part of its merchant education program. Two current publications geared specifically toward card-present merchant fraud prevention and data security include:

- *Card Acceptance Guidelines for Visa Merchants*
- *What to Do If Compromised, Version 4.0*

Both are available as downloadable PDF files.

For More Information

If you have questions or need additional information, please contact your acquirer.