



# Visa Merchant Best Practice Guide for Cardholder Not Present Transactions



## Table of Contents

<b>Section 1</b>	<b>About This Guide</b>	<b>03</b>
<b>Section 2</b>	<b>Merchant Procedures</b>	<b>05</b>
<b>Section 3</b>	<b>Authorisation</b>	<b>07</b>
	Authorisation Procedures	07
	Special Authorisation Procedures for CNP Transactions	07
	Merchant Authorisation Practices	07
<b>Section 4</b>	<b>Authentication and Verification</b>	<b>09</b>
	Authentication and Verification Services	09
	Verified by Visa (VbV)	09
	Card Verification Value 2 (CVV2)	09
	Address Verification Service (AVS)	09
<b>Section 5</b>	<b>Risk Management</b>	<b>11</b>
	Limiting Exposure to Risk	11
	Fraud Screening	12
	Possible Risk Indicators	12
<b>Section 6</b>	<b>Dispute Avoidance and Management</b>	<b>15</b>
	Avoiding Unnecessary Chargebacks	15
	Chargeback management tips for CNP merchants	15
	Chargebacks and merchant liability	17
<b>Section 7</b>	<b>Additional Resources</b>	<b>19</b>

# Section 1: About This Guide

*This guide is intended to offer advice to merchants accepting Visa transactions in the card not present (CNP) environment. This is defined, not by the goods or services sold by the merchant, but by the channel used to complete the transaction.*

Transactions are usually completed via internet, mail or telephone orders, from merchandise displayed in a catalogue, television sales via 'home shopping' networks or infomercials and telemarketing.

Payment cards are particularly suited for CNP environment because they provide a method for the merchant to obtain immediate payment for the purchase. They also provide an easy method for paying for international purchases, thus providing you with an opportunity to reach global markets. However, while doing business in the CNP environment provides distinct advantages for merchants, it also presents specific challenges that do not occur in the card present environment.

When a merchant sells goods or services to a cardholder in person, the opportunity exists to verify the authenticity of the card. As a result, processing card present environment transactions is a straightforward procedure, with minimal risk of associated fraud attached to the transaction. However, the CNP environment, presents particular problems for merchants, in terms of fraud detection and prevention because validating the card and authenticating the cardholder is not easily done.

Despite these challenges, doing business in the CNP environment can be very profitable principally because it allows you to sell goods and services far beyond your immediate location, lowers your overheads, and provides a very convenient method to cardholders for shopping as they can review items in a catalogue or on the internet at leisure and place orders at any time.

**Note:** This document is published as a best practices guide only. Please refer to your Acquiring Bank or payment service processor for more details of specific regulations and guidelines for operating your merchant account.



# Section 2: Merchant Procedures



When processing a CNP transaction, you should ensure that you obtain at least the following information from the cardholder:

- > Account number
- > Cardholder name as it appears on the card, if present
- > Expiration date as it appears on the card
- > Cardholder's billing address; the address that appears on the billing statement
- > Shipping address (if applicable); the address where the merchandise will be shipped (may be the billing address)
- > CVV2 (if you participate in the CVV2 service)

For telephone orders and Internet, you should also note the following information:

- > Cardholder contact information, such as telephone number or e-mail address
- > Time and date of the order
- > Details of the conversation

For mail/fax orders, it is advisable to obtain the cardholder's signature on the order form.

If you are processing an electronic commerce transaction and are enrolled for the Verified by Visa (VbV) service, then you should also indicate that VbV occurred by the use of the relevant Electronic Commerce Indicator (ECI) value. More information on VbV can be found in section 4.

In addition, you should always keep copies of order forms and obtain proof of delivery of merchandise to the address specified by the cardholder.

# Section 3: Authorisation



## Authorisation Procedures

When an Issuer approves an Authorisation request, it indicates that the account exists and is in good standing (i.e., that it has not been reported lost or stolen, or is not closed) and that the cardholder has sufficient funds in the account to make the purchase at the time the Authorisation request is made.

However, an Authorisation does not authenticate the cardholder or verify the card. Neither does it guarantee that the address provided by the cardholder is correct, or that the genuine cardholder participated in the transaction.

The requirement for the merchant to obtain Authorisation for a CNP transaction depends on the following factors:

- > **Transaction type** – Some types of transactions, such as electronic commerce and recurring transactions must always be authorised
- > **Floor limit** – Authorisation is required when the transaction amount is above the merchant's floor limit. You should check the relevant floor limit for your business with your Acquiring Bank.

## Special Authorisation Procedures for CNP Transactions

In general, an Authorisation is valid only when it is obtained on the transaction date. However, special Authorisation procedures exist for CNP transactions when goods will be shipped to the cardholder. The merchant may obtain Authorisation on any day up to 7 calendar days prior to the transaction date. For CNP transactions, the transaction date is the date that the merchandise is shipped, not the date that the cardholder placed the order.

The Authorisation is also valid if the transaction amount is within 15% of the authorised amount, provided that the additional amount represents shipping costs.

Regardless of the floor limit, Visa recommends that merchants obtain Authorisation for all CNP transactions. This practice is a useful safety measure that may prevent the merchant from becoming the victim of a fraudulent transaction.

## Merchant Authorisation Practices

In the event that you receive a decline response to the Authorisation request, you should not complete the transaction. Instead, you should investigate further to eliminate fraud and contact the cardholder to report the status and obtain an alternative card number. However, in some cases, contacting the cardholder may not be practical, and merchants occasionally make subsequent attempts to obtain Authorisation. Visa does not condone this practice as if you do make subsequent Authorisation requests, and receive an approval response you may still be subject to a chargeback for declined Authorisation.

# Section 4: Authentication and Verification



## Authentication and Verification Services

Visa currently provides three services for authenticating the card in the CNP environment:

- > Verified by Visa (VbV)
- > Card Verification Value 2 (CVV2)
- > Address Verification Service (AVS)

### Verified by Visa (VbV)

Verified by Visa (VbV) enables Issuers to authenticate the identity of cardholders registered in the service when making transactions over the Internet. When a cardholder makes a purchase at a merchant participating in VbV, software at the merchant's site recognises whether the card being used for payment is registered for VbV. If it is, a VbV screen appears and the cardholder is prompted to enter a password that was created at the time the card was registered. The Issuer then validates the cardholder's identity and sends a response to the merchant indicating that he can proceed with the Authorisation.

VbV, therefore, allows authentication of the cardholder at the time of purchase and consequently reduces the risk of fraud and helps towards the elimination of costs related to fraudulent transactions.

For merchants, VbV offers protection against fraudulent chargebacks even where the cardholder and/or the Issuing bank are not participating. VbV merchants may also benefit from a possible reduction in merchant fees from their acquirer.

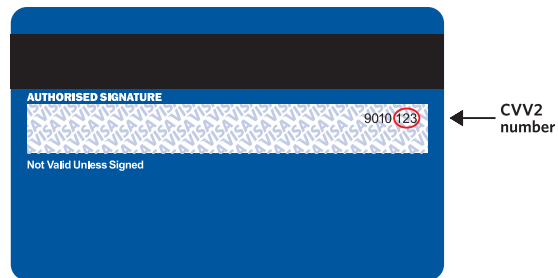
Although VbV offers an excellent anti-fraud tool, for maximum protection Visa recommends that you still continue to employ the best practices contained in this guide including using Cardholder Verification Value 2 (CVV2) alongside VbV.

For more detailed information about Verified by Visa, visit <http://www.visaeu.com/acceptingvisa/sellingonline.html> and refer to your Acquiring Bank.

### Card Verification Value 2 (CVV2)

The Card Verification Value 2 is a three-digit code printed on the signature panel on Visa cards. The CVV2 code helps validate that the cardholder is making a purchase with a genuine card that is linked to a legitimate account. All Visa cards must contain a CVV2 code.

Visa studies indicate that CVV2 is an effective deterrent to fraud in the CNP environment and can reduce fraud in some environments by more than 60%.



### Address Verification Service (AVS)\*

The Address Verification Service (AVS) helps merchants to validate elements of the cardholder's billing address with the Issuer. It is a significant service that can help you when determining whether a transaction is valid.

AVS is currently being used in a limited number of countries. In the countries where it is used, it has proven to be an effective inhibitor to fraud in the CNP environment. Used in combination, CVV2 and AVS can help merchants reduce fraudulent transactions from entering the system.

**\*Note:** In Europe at present, AVS is only available in the United Kingdom

# Section 5: Risk Management



## Limiting Exposure to Risk

Sound business policies and practices can help limit your exposure to fraud. Visa recommends that merchants doing business in the CNP environment implement the following best practices:

- > **Obtain an Authorisation** for all transactions, even if the transaction amount is below the floor limit. Authorisation tells you that the account is valid, in good standing, and has the funds available to make the purchase. Checking the Exception File or Combined Warning Bulletin only tells you whether or not the account is listed.
- > If participating in the CVV2 service, **obtain the CVV2 code** from the cardholder. An Issuer-validated CVV2 code is a good indicator that the card is genuine.
- > Where available, **verify the cardholder's billing address via the AVS**, which helps you to validate the cardholder's billing address directly with the Issuer. Where the delivery address is different from the valid statement address then you should take extra care.
- > **Maintain a history of cardholder's previous purchases.** Fraud is less likely to occur when the cardholder and merchant have a long term (greater than six month) relationship.
- > **Establish maximum amounts** that you will allow to be spent by an individual customer or on an individual card.
- > **Determine the frequency of transactions** from the same cardholder. Regular purchases over time, is generally normal activity. However, many transactions in a short period of time may indicate suspicious activity. This type of monitoring is key to detecting and mitigating fraud activity in the merchant's system. Transactions should be monitored by card number and delivery address. Where above-average velocities are seen on either of these criteria then additional investigations should be undertaken.
- > **Maintain records of shipping addresses** used by the cardholder. Merchandise shipped to the same address is normal, while purchases shipped to an assortment of addresses are suspicious although they could still be genuine.
- > **Confirm the purchase with the cardholder.** For high value items, and after the order has been placed, you may want to consider calling the cardholder to confirm the purchase although you should independently verify the phone number whether by directory enquiries or reference to a previous genuine order.
- > For electronic commerce transactions, always authenticate the cardholder using the **Verified by Visa** service and continue with your other fraud prevention and detection activities.
- > **Maintain a grey list** including records of chargebacks or disputes by delivery address. Where you have had previous problems at that address any subsequent transactions are more likely to be subject to problems.

## Fraud Screening

There are a wide variety of fraud screening services and practices available that will help you assess the risk of a transaction and increase the likelihood that the person making the transaction is the legitimate cardholder with a valid card. Fraud screening tools may be developed internally by you or your Acquirer, or may be purchased from a third party.

The following best practices will help you reduce the risk of fraud:

- > **Implement fraud screening tools** to identify high-risk transactions or patterns of transactions
- > **Do not process transactions with high-risk characteristics**, such as:
  - Transactions with data that matches those stored on grey lists.
  - Transactions that exceed velocity limits and controls
  - Transactions that generate either an AVS or CVV2 mismatch
  - Transactions that fit high-risk profiles
- > **Verify the cardholder's address** when a transaction generates an AVS mismatch by reference to voters roll information, local directories or direct with the cardholder.
- > **Screen for high-risk shipping addresses**, such as mail drops, post office boxes, prisons, hospitals, etc.
- > **Monitor for orders placed with multiple and specifically sequential card numbers or a disproportionate number of orders from one issuer.** These could indicate fraudulent behaviour.

- > **Provide greater scrutiny to international transactions.** Assess risk based on type of goods purchased, the transaction amount, the country where the card was issued, and the country where the merchandise is to be shipped. Your Acquirer should be able to offer help with this.

## Possible Risk Indicators

Visa recommends merchants put into place in-house policies and procedures for handling irregular or suspicious transactions (for example, unusually large orders). Sales staff should be trained to recognise suspicious orders and given clear instructions on the steps they should take to verify these transactions. Experience suggests that there are certain characteristics that can be tip-offs to possible fraud. One of these characteristics is rarely an indication of fraud. However, when several are present in the same purchase, it is much more likely to be a fraudulent transaction.

### Possible Risk Indicators

- > First time customer
- > High value orders or orders that are larger than normal
- > Customer hesitates over personal details
- > Customer requests urgent delivery
- > Ordering randomly or in multiples
- > Providing different ship-to and billing addresses
- > Paying with multiple cards

If one or more of the following indicators is present in the transaction, it may indicate increased risk:

- > **First time customers** - The risk of fraud is less when dealing with repeat customers
- > **Large orders** - Orders that are larger than normal may indicate fraud. Also high value purchases for items such as jewellery or electrical goods are often the target for fraud as they can easily be resold. Greater vigilance is required for these types of transaction.
- > **Multiple orders** - Orders consisting of several purchases of the same item may arouse suspicion



- > **Suspicious card combinations** – a variety of payment card combinations might give rise for concern and further investigation, for example:
  - a. transactions made with cards that have similar account numbers
  - b. orders shipped to a single address, but purchased with various cards
  - c. multiple transactions on a single card over a very short period of time, or,
  - d. multiple transactions made with several cards with a single billing address, but multiple shipping addresses
  - e. a single transaction in which the customer wants to pay with multiple cards. More than one or two cards may well indicate a fraudulent transaction.
- > **Hesitation.** Beware of customers who hesitate or seem uncertain when giving personal information, such as a postcode or the spelling of a street or family name. This is often a sign that the person is using a false identity.
- > **Rush orders** – Urgent requests for quick or overnight delivery – the customer who ‘needs it yesterday’ – are another sign of possible fraud. While often perfectly valid, rush orders are one of the common characteristics of ‘hit and run’ fraud schemes aimed at obtaining merchandise for quick resale.
- > **Random orders** – Watch out also for customers who do not seem to care if a particular item is out of stock (“You don’t have it in red? What colours do you have?”) or who order haphazardly (“I’ll take one of everything!”). Again, orders of this kind may be intended for resale rather than personal use.

- > **Suspicious shipping address** – Scrutinise 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. In addition, merchants should keep lists of postcodes where high fraud rates are common and verify any order that has a ship-to address in these areas. If your business does not typically service foreign customers, use caution when shipping to international addresses – particularly if you are dealing with a new customer or a very large order. Also be on the lookout for orders with requests for delivery outside your own market, unless this is typical for the type of goods being sold.

If fraud is suspected, you should contact the customer and ask for additional information to verify the order. Validate telephone numbers with addresses and check lists related to previous chargeback problems, etc.

The following steps may help to verify suspect transactions:

- > Ask the customer for the name of the Issuing Bank shown on the card or for the printed four-digit number on the face of the card.
- > Check the customer’s personal information. Request day and evening telephone numbers and verify them through directory assistance or by calling the customer directly. If possible, you should also compare the billing and ship-to address on the order with the address you used for mailing the customer any catalogues or other marketing materials.
- > Separately confirm the order with the customer. Send a note to the customer via his/her billing address, rather than the ‘ship to’ address.

Telephone Order employees who request additional information to verify orders must do so in a conversational tone so as not to arouse the customer’s suspicions. If the customer hesitates or asks why the information is needed, simply say that you are trying to protect cardholders from potential fraudulent activity.

Merchants delivering goods should:

- > Treat the sale as a Card Present transaction if a customer collects the goods in person
- > Be wary of customers who do not question additional costs
- > Treat international transactions with caution because it is difficult to confirm details of customers in other countries
- > Consider secure delivery through a courier company for high-value items or for delivery addresses that seem suspicious.



# Section 6: Dispute Avoidance and Management



## Avoiding Unnecessary Chargebacks

- > Act quickly when a cardholder reports a problem
- > Process refunds quickly
- > Follow up with the cardholder
- > Respond promptly to requests for transaction receipts

While disputes are rare for most merchants, they are inevitable at some point in time. Not dealing with them adequately can lead to chargebacks, which, in turn, can result in loss of business and revenue. To minimise losses from chargebacks, you must establish procedures and practices for avoiding unnecessary chargebacks, as well as an in-depth understanding of your rights and responsibilities in the chargeback process.

## Chargeback management tips for CNP merchants

The following suggestions may be useful in preventing potential chargebacks.

- > **Expired card** - If the expiration date reported or entered by the cardholder precedes the transaction date, the card is expired and as such invalid. If you do not obtain authorisation, the transaction may be charged back as 'expired or not authorised'. **Note:** A card is valid until the last day of the month indicated on the card. For example, 'Valid until 04-04' means the card is valid until the 30th day of April, 2004, but expires on May 1st, 2004.
- > **Declined authorisation** - Merchants should not complete the transaction if the authorisation was declined. Similarly, for VbV transactions, the merchant should not proceed where the authentication has failed.
- > **Submit transactions only once** - Make sure transactions are deposited and files are transmitted only once. If the merchant copy and the financial institution copy are deposited, or if the same transaction is deposited with more than one financial institution, this may lead to chargebacks due to 'Duplicate Processing'. The same rule applies when transaction information files are transmitted more than once.
- > **Communicate your return, reimbursement and service cancellation policies** - If you have a return, reimbursement and cancellation policy in place, communicate this policy to the cardholder at the time the transaction is completed, or include this information in clear terms on your website. Failure to communicate these policies will be detrimental to you if the customer decides to return the merchandise or cancel the services.
- > **Transaction receipt deposits** - It is always beneficial for the merchant to deposit or submit transaction information as soon as possible, preferably within a period of one to five days from the transaction date. Retaining them any longer may lead to chargebacks due to 'Late Presentment'.
- > **Deposit or submit credit transactions quickly** - It is advisable to deposit or submit the credit information file to your financial institution as soon as possible, preferably the same day the credit transaction is generated. If credits are not processed quickly, this may lead to a chargeback due to 'Credit Not Processed'.
- > **Customer complaints** - Act promptly when a cardholder contacts you about a problem. If customer complaints are addressed at an early stage, unnecessary chargebacks may be avoided.

- > **Fulfil copy requests** – It is important to always fulfil requests for copies of receipts quickly. Send a legible copy of the requested receipt or file along with the transaction information to your financial institution. If requests are incompletely fulfilled or not fulfilled within the specified time limit, this will invariably lead to a chargeback due to 'Nonfulfilment of Copy Request'. The transaction receipt should contain all the information available about the transaction, such as:
  - Account number
  - Card expiration date
  - Cardholder name
  - Transaction amount
  - Transaction date
  - Authorisation code
  - Description of the goods or services
  - Merchant name
  - Merchant contact information
  - Billing address
  - Shipping address
  - Address verification response code
  - CVV2 response code
  - Cardholder telephone number or email address.
- > The information needed to respond to the Request For Information (RFI) for e-comm transaction are:
  - Merchant Name
  - Merchant Location (On Line Address)
  - Account Number (the clearing logs if the number is truncated)
  - Cardholder Name
  - Transaction Date
  - Transaction Amount
  - Transaction Currency
  - Authorisation Code
  - Description Of Merchandise or Services sold
- > **Recurring transaction cancellation requests** – If the customer requests the cancellation of a transaction that is periodically billed (monthly, quarterly or annually), it is important to always respond to the request and cancel the transaction immediately or as specified by the customer. As part of your customer service, notify the cardholder in writing (by regular or electronic mail) that the service, subscription or membership has been cancelled, as well as the cancellation date. Failure to respond to cancellation requests will almost invariably lead to a chargeback.
- > **Ship merchandise before depositing transaction** – Merchants should not deposit or submit the transaction information file until the ordered merchandise has been shipped. If the customer sees a transaction on his or her monthly Visa statement before the merchandise is received, this may lead to a chargeback that could have been prevented due to 'Non-Receipt of Merchandise'.
- > **Recognisable merchant name** – It is critical for customers to be able to recognise transactions in their Visa statements to avoid potential disputes. When the cardholder cannot recognise transactions, he or she generally questions the Issuer or disputes the transaction. The card Issuer may then request a copy of the transaction receipt to help the customer identify it. Sometimes these questions lead to a chargeback. To ensure customers are able to recognise the name of the merchant outlet, consider taking the following actions:
  1. Ask your financial institution to show you the way your business is identified in the interchange record (your name will appear in this way in the Issuer processing system when the transaction is posted to the cardholder's Visa account). If the name is incorrect or may be confusing for cardholders, ask the institution to change it.
  2. Verify the name printed by the financial institution in your statements to ensure it is the same as the name in your customer receipts. (Generally, the name used for settlement purposes must be the same one you use in the signs that identify your business.)
  3. Charge a purchase to your card at each of your outlets and verify the name and address shown in the Visa monthly statement. Will your customers recognise these transactions?

## Chargebacks and merchant liability

There are four main reasons for chargebacks in Card Absent transactions.

- > The most common involves fraud where the cardholder claims that he did not participate in the transaction.
- > Failure to process a credit for returned merchandise is another reason for disputes.
- > Non-receipt of merchandise can also lead to disputes.
- > Visa introduced a chargeback right for 'Transaction Not Recognised' in October 2004. This chargeback is exercised when a cardholder claims that he does not recognise a transaction.

It is important for merchants to understand their rights and responsibilities with respect to Chargebacks. However, as chargeback rules and merchant liability vary by market Visa advises that you obtain information from your Acquirer about the rules applicable to you.

# Section 7: Additional Resources



The information contained in this document is intended only as a guide for merchants and is not a definitive set of instructions. Visa recognises that business practices vary across different industry types and in different markets whereby some of the suggestions and recommendations may be different. To make the most of your Visa business, Visa strongly recommends that you also consult with your Acquiring Bank and payment processor for further more in depth information.