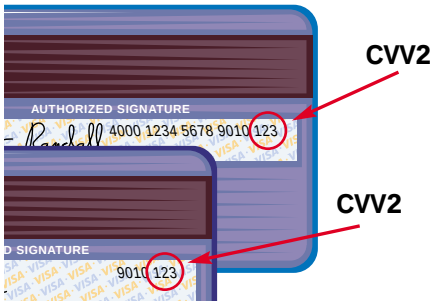
VISA CARD VERIFICATION VALUE 2 (CVV2) MERCHANT GUIDE

A Tool for Understanding CVV2 for Greater Fraud Protection

CVV2—A unique feature that allows you to authenticate the Visa card.

What is CVV2?

CVV2, which stands for Card Verification Value 2, is an important security feature for merchants who accept Visa cards as payment over the telephone or online. Located on the back of all Visa cards, the CVV2 consists of the last three digits printed on the signature panel.



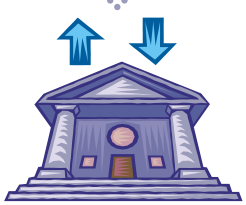
In the card-not-present sales environment, CVV2 is an excellent tool for verifying that the customer has a legitimate Visa card in hand at the time of the order.

How Does CVV2 Work?

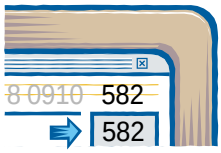
From start to finish—CVV2 works as follows:

The **customer** contacts the merchant to place an order.

The **merchant** asks the customer for the CVV2 three-digit code and sends it to the card issuer as part of the authorization request.



The **card issuer** checks the CVV2 code to determine its validity, then sends a CVV2 result code back to the merchant along with the authorization decision.



Before completing the transaction, the **merchant** evaluates the CVV2 result code, taking into account the authorization decision and any other relevant or questionable data.

Why Implement CVV2?

Merchants who use CVV2 benefit in a number of ways:

✔ **Enhanced Fraud Protection**

Because card-not-present merchants are at greater risk for stolen account number schemes, you need to be diligent in your fraud control efforts. CVV2 can help a merchant differentiate between good customers and fraudsters who operate anonymously. It allows you to make a more informed decision before completing a non-face-to-face transaction.

✔ **Reduced Chargebacks**

Using CVV2 potentially reduces fraud-related chargeback volume. Reduced fraud-related chargebacks translate into maximized profitability.

✔ **Improved Bottom Line**

For card-not-present merchants, fraudulent transactions can lead to lost revenue and can also mean extra processing time and costs, which often narrow profit margins. CVV2 complements your current fraud detection tools to provide a greater opportunity to control losses and operating costs.

Who Needs to Know About CVV2?

Anyone involved with CVV2 should be well-versed and trained in its usage. This typically includes:

- ✔ Sales terminal software and screen management,
- ✔ Order-takers/sales associates,
- ✔ Risk or fraud management, and
- ✔ Customer service representatives

To assist you in your CVV2 training and communication efforts, a CVV2 Processing Quick Reference tool has been included on the next page of this guide.

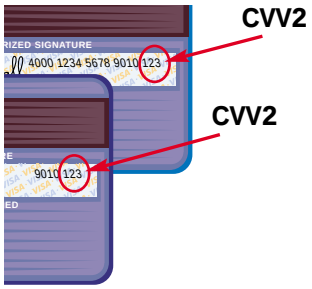
VISA®

CVV2 Processing Quick Reference

Here's a tool to help ensure that the proper CVV2 steps are followed during the sales order process.

1. Ask the customer for the account number and expiration date on the front of the card.

2. Instruct the customer to turn the card over and read or enter the last three numbers printed in the signature panel on back of the card. Explain that these are the three digits that immediately follow the full Visa card account number (all 16 digits) or the partial account number (just the last 4 digits).



3. Send one of the following CVV2 presence indicators along with other required authorization data (i.e., account number, expiration date, and transaction amount).

The CVV2 presence indicator is an important tracking mechanism that allows merchants to better understand the characteristics of non-face-to-face transactions.

IF:	SEND THIS INDICATOR TO THE CARD ISSUER:
You have chosen not to submit CVV2	0
You have included CVV2 in the authorization request	1
Cardholder has stated CVV2 is illegible	2
Cardholder has stated CVV2 is not on the card	9

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

RESULT:	ACTION:
M – Match	Complete the transaction (taking into account all transaction characteristics and any questionable data).
N – No Match	View the "No-Match" as a sign of potential fraud and take it into account along with the authorization response and any other questionable data. Potentially hold the order for further verification.
P – CVV2 request not processed	Resubmit the authorization request.
S – CVV2 should be on the card, but cardholder has reported to the Merchant that there is no CVV2	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 in the signature panel.
U – Issuer does not support CVV2	Evaluate all available information and decide whether to proceed with the transaction or investigate further. Uncertified card issuers lose chargeback rights for Fraudulent Mail Order/Telephone Order (MO/TO) transactions when CVV2 is included in the authorization message.

5. If you receive an authorization, but suspect fraud:

- Call the customer with any questions.
- Ask for additional information (e.g., bank name on front of card).
- Separately confirm the order by sending a note to the customer's billing address.

6. Contact your merchant bank to report suspicious activity.

What Else Should I Know About CVV2 and Fraud Detection?

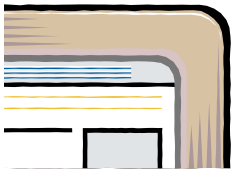
For card-not-present merchants, CVV2 is highly effective when it comes to minimizing the risk of accepting a stolen or compromised Visa account number. It is even more powerful, however, when used with the right combination of controls.

For additional fraud detection capability, consider these tools:

✔ **Visa Address Verification Service (AVS)** allows card-not-present merchants to check a Visa cardholder's billing address with the card issuer. The merchant includes an AVS request as part of the authorization and receives a result code indicating whether the address given by the cardholder matches the address on file with the card issuer.

✔ **Verified by Visa** lets e-Commerce merchants validate a cardholder's ownership of an account in real time during a transaction. When a registered "Verified by Visa" cardholder clicks "buy" at the checkout of a participating merchant, the merchant server recognizes the Visa card and prompts the cardholder to enter a password, which is forwarded to the card issuer. Within seconds, the issuer confirms the cardholder's identity and verifies the Visa account.

✔ **CyberSource Advanced Fraud Screen Enhanced by Visa** is a card-not-present risk management tool that estimates— in real time—the level of risk associated with each transaction and provides merchants with risk scores. These scores enable merchants to more accurately identify potentially fraudulent orders.



Your merchant bank can give you the details on how these three tools complement CVV2 and add to your level of fraud protection.

Should Merchants Save CVV2 Codes?

To protect CVV2 from being compromised, NEVER keep or store a Visa card's CVV2 code once a transaction has been completed. Such action is prohibited and could result in fines.

What Do I Need to Do to Start Using CVV2?

If you have questions or would like the technical requirements for implementing Visa's CVV2 security feature, contact your merchant bank.

What Other Visa Resources are Available for Card-Not-Present Merchants?

Visa offers a number of risk management materials as part of its merchant education program. Current publications geared toward card-not-present merchant needs include the following:

- **Merchant Guide to the Visa Address Verification Service (AVS)**–VBS 07.03.01
- **Chargeback Management Guide for Visa Merchants**–VBS 05.01.02
- **Visa E-Commerce Merchants' Guide to Risk Management**–VBS 05.02.02
- **CyberSource Advanced Fraud Screen Enhanced by Visa**–VBS 03.01.02
- **Protect Your Virtual Storefront**–VBS 01.04.01

You can ask your merchant bank to order these Visa publications for you, or order them directly by calling the Visa Fulfillment Center at 800-847-2311.