



Fraud Control Basics

Card Not Present

Extra protection when there's no card

Card-not-present (CNP) merchants must take extra precaution against fraud exposure and associated losses. Anonymous scam artists bet on the fact that many Visa fraud prevention features do not apply in this environment.

Follow these recommendations to help prevent fraud in your card-not-present transactions.

On these pages

- Visa CNP payment acceptance
- 12 potential signs of CNP fraud
- Visa CNP fraud prevention tools

Visa CNP payment acceptance

Take these steps to accept Visa CNP payments:

1. Obtain an authorization.
2. Verify the card's legitimacy:
 - Ask the customer for the card expiration date, and include it in your authorization request. An invalid or missing expiration date might indicate that the customer does not have the actual card in hand.
 - Use fraud prevention tools such as Visa's Address Verification Service (AVS), Card Verification Value 2 (CVV2), and Verified by Visa.
3. Look for general warning signs of fraud (listed below).
4. If you receive an authorization, but still suspect fraud:
 - Ask for additional information during the transaction (e.g., request the financial institution name on the front of the card).
 - Contact the cardholder with any questions.
 - Confirm the order separately by sending a note via the customer's billing address rather than the "ship to" address.

To report suspicious activity, contact your merchant financial institution.

12 potential signs of CNP fraud

Keep your eyes open for the following fraud indicators. When more than one is true during a card-not-present transaction, fraud might be involved. Follow up, just in case.

1. **First-time shopper:** Criminals are always looking for new victims.
2. **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchase.
3. **Orders that include several of the same item:** Having multiples of the same item increases a criminal's profits.
4. **Orders made up of "big-ticket" items:** These items have maximum resale value and therefore maximum profit potential.

5. **“Rush” or “overnight” shipping:** Crooks want these fraudulently obtained items as soon as possible for the quickest possible resale, and aren’t concerned about extra delivery charges.
6. **Shipping to an international address:** A significant number of fraudulent transactions are shipped to fraudulent cardholders outside of the U.S. Visa AVS can't validate non-U.S., except in Canada and the United Kingdom.
7. **Transactions with similar account numbers:** Particularly useful if the account numbers used have been generated using software available on the Internet (e.g., CreditMaster).
8. **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.
9. **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.
10. **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.
11. **In online transactions, multiple cards used from a single IP (Internet Protocol) address:** More than one or two cards could definitely indicate a fraud scheme.
12. **Orders from Internet addresses that make use of free e-mail services:** These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

Visa CNP fraud prevention tools

Appropriate preventive action can help reduce fraudulent transactions and potential customer disputes. Make use of these Visa tools and controls to verify the legitimacy of the Visa cardholder and the card in every card-not-present transaction.

Tool	Description
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 Issuer.
Card Verification Value 2 (CVV2)	<p>Is a three-digit number imprinted on the signature panel of Visa cards to help card-not-present merchants verify that the customer has a legitimate card in hand at the time of the order. The merchant asks the customer for the CVV2 code and then 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 back to the merchant along with the authorization. CVV2 is required on all Visa cards.</p> <p>To protect CVV2 data from being compromised, Visa U.S.A. Inc. Operating Regulations prohibit merchants from keeping or storing CVV2 numbers once a transaction has been completed.</p>
Verified by Visa (VbV)	Enables e-commerce merchants validate a cardholder's ownership of an account in real-time during an online Visa card transaction. When the cardholder clicks "buy" at the checkout of a participating merchant, the merchant server recognizes the registered Visa card and the “Verified By Visa” screen automatically appears on the cardholder’s desktop. The cardholder enters a password to verify his or her identity and the Visa card. The Issuer then confirms the cardholder’s identity.