



And, as of April 2005, if a merchant submits the CVV2 value for authentication to the cardholder's Issuer, and the Issuer does not participate in CVV2 validation, the merchant will be protected from any potential fraudulent transactions.

For more information on how you can start using CVV2 in your business, speak to your Visa Acquirer.

What can you do to protect your business against card-not-present fraud?

- Sign up to participate in the Verified by Visa program. For more information, visit www.visa.ca/verified.
- When taking orders over the phone, or over the Internet, ask the customer for the card expiration date and include it in your authorization request. An invalid or missing expiration date can be an indicator that the person on the other end does not have the actual card.
- Use fraud detection tools such as CVV2 as part of the authorization process.
- Be on the lookout for purchases where multiple cards are used from a single IP (Internet Protocol) address, or those where orders are charged to multiple cards but are shipped to the same address - these could signal fraudulent activity.
- Be alert for transactions with several of the following characteristics: first-time shopper, larger than normal orders, orders consisting of several of the same item, orders made up of 'big-ticket' items, orders shipped 'rush' or 'overnight', and orders shipped to an international address.

HACKING

Today criminals are increasingly becoming tech-savvy and have found ways to hack into a company's computer system to gain access to confidential customer information. By hacking into your system, criminals can not only gain access to customer information, but they can also obtain sensitive information about your business.

What is Visa doing to help safeguard your system?

Visa Account Information Security Program (AIS)

AIS is a global program requiring merchants to make their virtual and physical environments more secure, thereby helping protect against hacks. This program provides merchants with an easy-to-use toolkit targeted at the protection of cardholder account and transaction data. The program includes global standards, a best practices guide, and a self-assessment questionnaire providing key information and requirements.

Recently, Visa aligned its AIS program with the security protection program run by other payment providers to provide a Payment Card Industry (PCI) set of data security standards. These standards were aligned to further ensure

the safe handling of card information and improve cardholder confidence. Merchants and service providers are now able to assess the status of their security by using a single set of security standards.

What can you do to protect your business against hacking?

- Ensure your business complies with the standards set out in the Visa AIS program. To learn more about the program, visit www.visa.ca/ais.
- Limit access by your employees to account data on a need-to-know basis.
- Develop in-house fraud detection programs, such as guidelines for staff on how to spot and report suspected fraudulent transactions.
- See if your business is fraud-proof. Take the merchant self-assessment quiz at www.visa.ca/securewithvisa.
- Install software to protect systems and data from viruses and update security software frequently.
- Immediately investigate and report to your Acquirer any suspected loss of account or transaction information.
- Encrypt data maintained on databases or files accessible from the Internet, and any data sent across networks.
- Securely destroy data when it is no longer needed for business reasons.
- Remove access to the network and the premises immediately for any employee who has left your business.
- Do not provide account data to someone over the phone - unless you are the one who initiated the call.

To learn more about recognizing, reporting and stopping fraud, visit:

www.visa.ca/securewithvisa

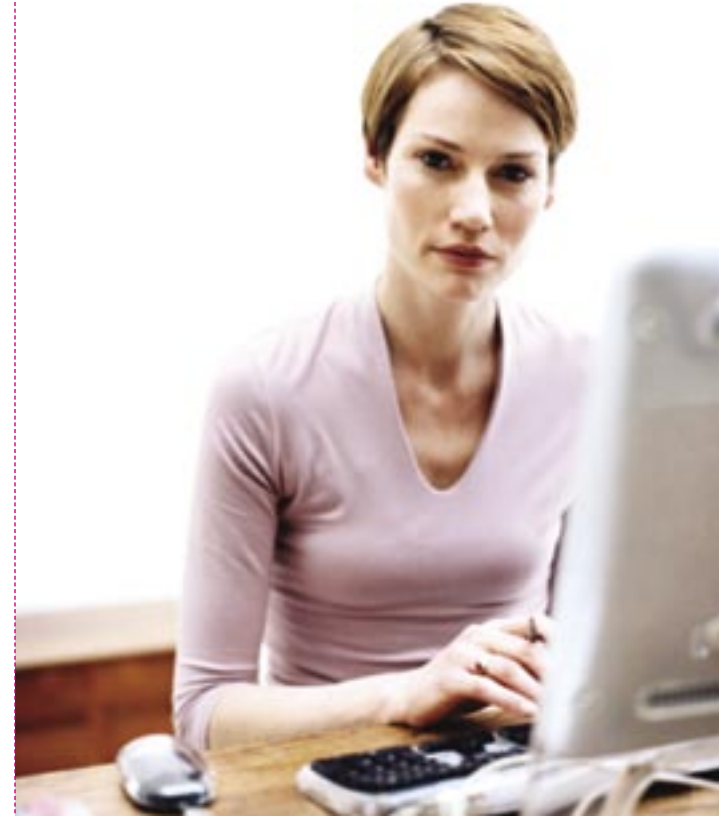


™ Trademark of Visa International Service Association; Visa Canada Association is a licensed user.



Credit Card Fraud:

A guide to help businesses
Recognize it. Report it. Stop it.



At Visa, we strive to offer the latest information to assist you in providing the safest, most secure transaction environment for you, and your customers.

We understand that security is important to both you and your customers, and we work closely with our Member financial institutions, law enforcement, and Acquirer Processors to help ensure a safe payment environment.

There are however, things that you as a merchant can do to help reduce your risk of becoming a target for fraud. This brochure provides information that will help you recognize credit card fraud, report it, and play a role in stopping it.

THE MANY FORMS OF FRAUD

Criminals use a number of tactics in an attempt to defraud legitimate businesses. Below are some of the things to watch out for:

COUNTERFEITING

What is counterfeiting?

Counterfeiting involves making replicas of legitimate credit cards by copying or “skimming” the data contained in a card’s magnetic stripe. Using this “skimmed” information, criminals manufacture phoney or counterfeit cards and use them for fraudulent purposes.

Counterfeiting represents a large portion of credit card fraud involving Canadian issued credit cards.

What is Visa doing to help prevent counterfeit fraud?

The VISA® Chip Card

Visa is working to bring Visa chip cards to cardholders. A chip card is a credit card that has a computer chip containing a microcomputer embedded into the card. In Canada, Visa leads the way in migration to chip cards. The microcomputer chip in a Visa card stores and processes data. Information on the chip card is virtually impossible to counterfeit and countries implementing chip have seen a reduction of up to 80% in counterfeit fraud. To find out more about what the Visa chip card, visit www.visa.ca/chip.

Visa card security features

One of the easiest ways to avoid fraud is to spot counterfeit cards before you process the transaction. Visa cards have a number of built-in security features designed to help merchants recognize a real card from a counterfeit one.

While processing a transaction, take the time to look over the card presented for payment and ensure it has the following security features.



Embossing: Is it clear and straight?

Four Printed Numbers: Do they match the first four numbers of the embossing?



Signature Panel: Does it bear the repeated word “VISA” in blue and gold at an angle?

What can you do to stop counterfeit fraud?

- Always check the card for key security features such as: embossing, and the repetition of the first four numbers printed on the card.

- Compare the signature. The signature on the receipt should match the signature on the back of the credit card.
- If you are ever suspicious about a card, call your authorization centre and ask for a “Code 10” authorization. An operator will tell you what to do. However, never do so at the risk of your own personal safety.
- Ensure all staff are educated on proper acceptance procedures.
- Know your employees. Check references or conduct background checks on all of your employees.

CARD-NOT-PRESENT FRAUD

What is card-not-present fraud?

This type of fraud is committed without the actual use of a card—for instance in online, phone or mail-order transactions—and is the fastest growing fraud category in Canada. Fraudsters particularly like this type of fraud because they do not have to be physically present to commit the crime.

What is Visa doing to help prevent card-not-present fraud?

Verified by Visa® Program

Verified by Visa (VbV) is a global program providing a new level of security for online transactions. VbV assists in protecting merchants from fraudulent transactions through the cardholders’ use of a password, which helps to ensure that the cardholder is in fact the person conducting the transaction. Since Verified by Visa addresses a key concern of online protection among consumers, becoming a VbV participating merchant can enhance your reputation as a merchant with a safe shopping site, and turn the “e-browser” into a loyal, repeat purchaser.

Online retailers who participate in the Verified by Visa program can receive protection from up to 70% of fraud related chargebacks.

Card Verification Value 2 (CVV2)

CVV2 is a three-digit security number imprinted on the signature panel of Visa cards. This three-digit number is used to help merchants validate that the customer has a genuine card in his or her possession during an Internet or Mail Order/Telephone Order (MOTO) transaction.

When taking orders in card-not-present environments, merchants can ask their customers for this number as a way to help verify the customer is in actual possession of the card. Visa issuers that provide a real-time check of the code to help merchants verify that the person making the purchase actually has the card in hand. If a purchaser only has the 16-digit credit card number and the expiry date, they may not be in actual possession of the card, signalling a potential fraudulent transaction.