Card-Not-Present Security

A Multi-layered Approach to Payment Card Security

A multi-layered approach to payment card security.

A recent research study revealed that *Visa*® cards are the most widely used payment method at Canadian websites, on the phone, or through the mail.*

Over 5 million *Visa* cardholders make one or more purchases every year without their card ever being present at the point of transaction.**

As with all credit card transactions, card-not-present transactions are susceptible to fraud. At Visa, security in today's prevalent card-not-present environment is a top priority.

Visa merchants play an important role in protecting the payment card system from fraud. That is why Visa has developed a layered approach to card security in the card-not-present environment. This layered approach has been developed to offer both merchants and consumers multiple checkpoints and "layers" of security with each one designed to stop fraudsters in their tracks.

With tools like the *Verified by Visa*® (VbV) program, the Account Information Security (AIS) program, the 3-Digit Code on the signature bar (CVV2), and the Address Verification Service (AVS) you can be confident that you are offering the highest level of security to your clients when they make online, phone or mail order purchases from you.

*ComScore Tracking, 2004.

**Visa Canada 2004/2005 Statistics.

Visa
Anti-Fraud Program

Account Information Security (AIS) Program

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

Address Verification Service (AVS)

This service verifies a cardholder's billing address information and provides a results code to the merchant that is separate from the authorization response code. As a merchant, you can then make an informed decision to continue with the transaction.

As of October 1, 2006, Issuers will be prohibited from exercising fraud-related chargebacks for Reason Code 83 (Non-possession of card) when the Issuer is not participating in the AVS program and does not respond to a merchant's request for verification.

3-Digit Code (CVV2)

The 3-Digit number (CVV2) is imprinted on the signature panel of *Visa* cards. These numbers are used to help merchants validate that the customer has a genuine card in his or her possession during an Internet or Telephone Order transaction.

As of April 1, 2005, Issuers will be prohibited from exercising fraud-related chargebacks for Reason Code 83 (Non-possession of card) when the Issuer is not participating in the 3-Digit Code program and does not respond to a merchant's request for verification.

Verified by Visa (VbV)

VbV is a global program providing an added level of security for online transactions. An innovative service for online merchants, the *Verified by Visa* service verifies cardholder identity in real-time so customers can shop more confidently and merchants can accept *Visa* cards with peace of mind.

Acronym Decoder

AIS – Account Information Security

AVS – Address Verification Service

VbV – *Verified by Visa*

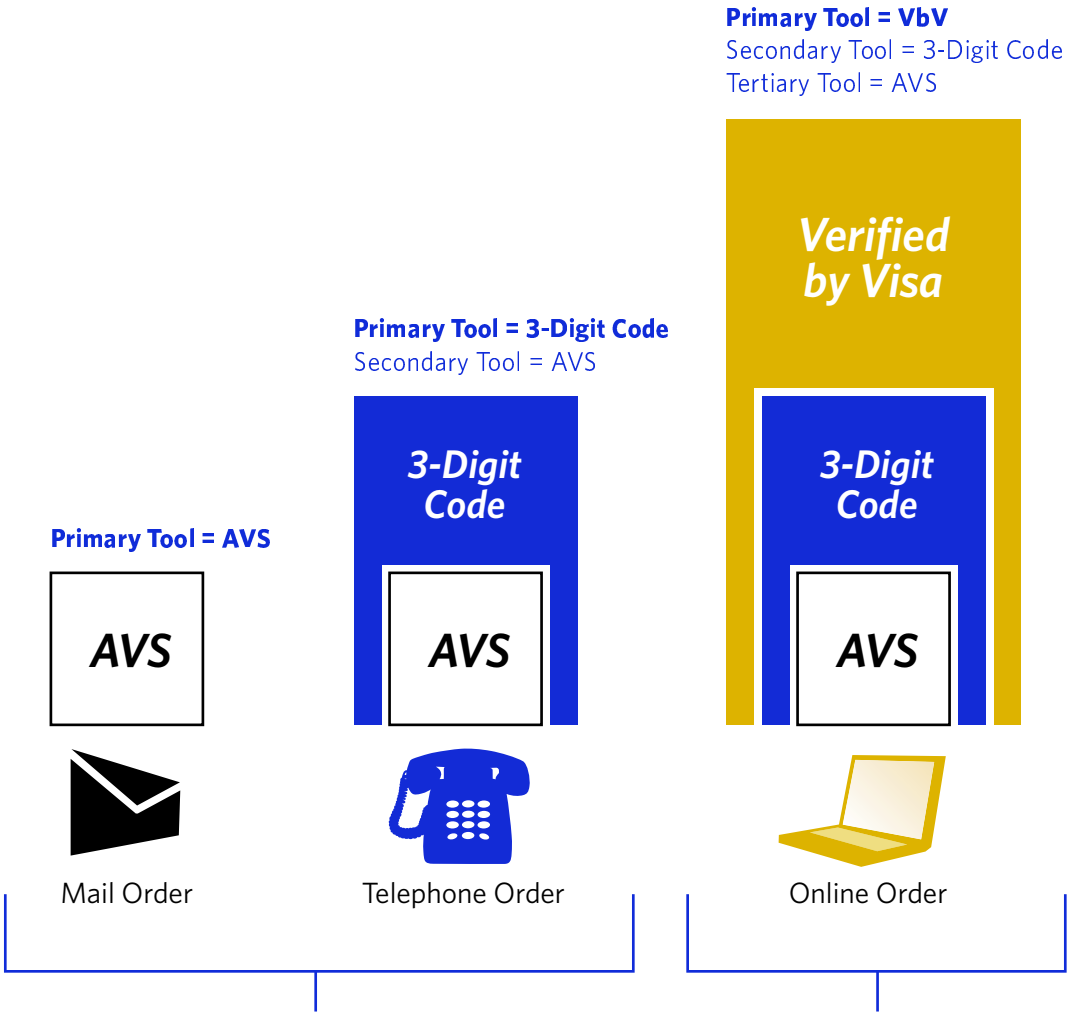
CVM – Card Verification Method

CVV2 – Card Verification Value 2

CNP – Card-Not-Present

PAN – Primary Account Number

A Layered Approach - By Channel



- Most complete merchant guarantee
- An Issuer platform that can evolve, as required
- Merchant can augment with 3-Digit Code, AVS layers for VBV limitations like Commercial Cards & optional activation

Fraud Prevention
For Your Business

The *Verified by Visa* service, the 3-Digit Code, and AVS are all designed to protect both merchants and cardholders from fraudsters. However, each product is designed with certain business types in mind. To find out which products are designed specifically for your business, read on.

If your business is:

Online: Your primary solution is the *Verified by Visa* service. *Verified by Visa* offers the best protection against fraud-related chargebacks, in allowing your customers to verify their identity at the time of the purchase, and by ensuring you are not accepting fraudulent cards at your Web site.

Telephone Order: The 3-Digit Code is added security for merchants accepting payments over the telephone. The 3-Digit Code is a security number imprinted on the signature panel of *Visa* cards. It enables merchants to ask for this unique three-digit code and provide a real-time check of the code to help merchants verify that the person making the purchase physically has the card in hand. If a purchaser only has the 16-digit credit card number and the expiry date, they may not have actual physical possession of the card, signaling a potentially fraudulent transaction.

Mail Order: AVS helps protect merchants and cardholders by checking a cardholder's billing address and/or postal code in real-time. AVS helps you, as a mail order merchant, make the decision about whether to complete a particular transaction. If a fraudster has obtained a card number from a receipt, or from a lost or stolen card, they will not have the billing address or postal code. AVS is processed through the VisaNet system, therefore verification in place of authorization is immediate.

Tips to Help You Prevent Fraud

We understand that both you and your customers are concerned about fraud and we work closely with our Member financial institutions, law enforcement, and merchant services providers 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 fraud target. These tips can help you to recognize and help stop payment card fraud.

Keep your eyes open for the following fraud indicators. When more than one of the following statements is true during a card-not-present transaction, fraud might be involved.

So, follow up, just in case.

1. **First-time shopper:** Criminals are always looking for new merchants to steal from.
2. **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, criminals need to maximize the size of their purchase.
3. **Orders that include several varieties 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:** Criminals want their 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 Canada/U.S.
7. **Transactions with similar account numbers:** May indicate the account numbers used have been generated using software available on the Internet.
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 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.

CyberSource Advanced Fraud Screen enhanced by Visa

As an extra layer of card-not-present security, Visa Canada has teamed up with CyberSource to offer *CyberSource Advanced Fraud Screen enhanced by Visa* to Canadian e-commerce merchants and merchant services providers.

What is it?

CyberSource Advanced Fraud Screen enhanced by Visa is the first e-commerce fraud detection system enabled with current worldwide fraud trend and global payment-card usage patterns that provides you with a real-time, accurate risk score.

What are the benefits?

It operates around the clock, 7 days a week, 24 hours a day. It effectively screens shoppers located anywhere in the world. It works with all payment cards. It is built on a system architecture that scales along with you as order volumes increase and your business grows. It has a centralized interface to give you the ability to build risk-decision strategies easily, and quickly accept, reject, and integrate payment authorization into the same strategy.

To learn more about this product, visit **www.cybersource.com**, or talk to your merchant services provider.

Verified by Visa® (VbV)

What is Verified by Visa?

The *Verified by Visa* (VbV) service is a global program designed to make shopping on the Internet safer and more secure for both shoppers and merchants.

Based on the 3-D Secure protocol, the VbV service verifies the authenticity of cardholders to participating merchants, ensuring that only the actual cardholder can use it to make purchases on the Internet.

Cardholders sign up for the VbV service through their issuing financial institution and choose their own personal password to authenticate themselves online.

How will VbV benefit an e-commerce site?

While e-commerce transactions on a secure Web site are generally safe, consumers have often been hesitant to use their credit cards online, resulting in untold lost sales. The VbV service allows cardholders to choose a password through their card issuer, and use it to authenticate themselves while making a purchase. This helps ensure that their card number cannot be fraudulently used at an e-commerce Web site.

Through the VbV password verification process, *Visa*® cardholders' identities are confirmed in real-time during checkout by the cardholder's financial institution. And since VbV addresses a key concern of online protection, it can enhance the merchant's reputation as a safe shopping site and turn the "e-browser" into a loyal repeat purchaser.

Designed to closely replicate a "card present" environment, VbV can reduce the risk of fraud and chargeback costs – with minimal impact to the current transaction process.

What is the process for the merchant?

Implementing VbV on an e-commerce site is done by the installation of a Visa certified Plug-in software module.

Once the customer has entered their payment card details, the e-commerce Web site passes control to the Plug-in software module. This module engages Visa's global *Verified by Visa* service to link together customers and their card Issuers.

Through Visa approved screen prompts (refer below) card Issuers are able to verify that the passwords entered by their cardholders are correct, and so provide merchants with immediate confirmation as to whether or not their transactions are protected from fraud-related chargebacks. This confirmation is returned to the merchant's e-commerce Web site by the Plug-in software module.

Verified by Visa® (VbV) cont'd

The possible outcomes of the Verified by Visa process and their implications for the merchant are outlined below:

Outcome of the Verified by Visa process	Implications for merchants
Cardholder is successfully authenticated	Merchant is protected from fraud-related chargebacks, and can proceed with authorization using Electronic Commerce Indicator (ECI) of '5'.
Card Issuer or cardholder is not participating in Verified by Visa	Merchant is protected from fraud-related chargebacks, and can proceed with authorization using Electronic Commerce Indicator (ECI) of '6'.
Card Issuer is unable to authenticate	Merchant is not protected from fraud-related chargebacks, but can still proceed with authorization using Electronic Commerce Indicator (ECI) of '7'. This condition occurs if the card type is not supported within Verified by Visa (e.g. Visa Commercial Card or prepaid gift card) or if the card Issuer experiences technical problems.
Cardholder failed to authenticate successfully	The customer has been unable to provide the card Issuer with the correct password and the transaction is therefore deemed to be fraudulent. The Merchant is not allowed to proceed with the transaction.

For more information, merchants should speak to their merchant services provider, or visit *www.visa.ca/verified*.

Account Information Security (AIS)

What is the Account Information Security Program?

Account Information Security is a mandated program that outlines a set of standards for the safe storage of cardholder information. The AIS program was designed to protect Visa® account and transaction information, safeguarding both the integrity of operations and the goodwill of cardholders.

How will the AIS program benefit merchants?

The AIS program was developed to define protection requirements for the management of sensitive account and transaction information in the Visa acceptance environment. The standards help merchants protect customer information from unauthorized access through an external breach (hack) or internal compromise. Merchants ultimately benefit by lowering their liability, building a compelling reputation for transaction safety, and eliminating the possibility of damaging negative publicity due to compromise.

The standards are designed to help merchants and institutions protect account information from unauthorized modification, disclosure, or destruction, thereby boosting consumer confidence and satisfaction. Examples of standards include those that address cryptographic operations, logical access controls, physical data protection, and network security. Standards address many key functional areas that influence the confidentiality, availability, and integrity of data.

How does a merchant become compliant?

Merchants should contact their merchant services provider for details regarding the assessment process and questions related to the Account Information Security Program.

See also *www.visa.ca/ais* for more information.

Other Information:

Payment Card Industry (PCI) – Recently, Visa aligned its Account Information Security (AIS) program with the Site Data Protection (SDP) security protection program run by MasterCard 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 requirements for both Visa and MasterCard.

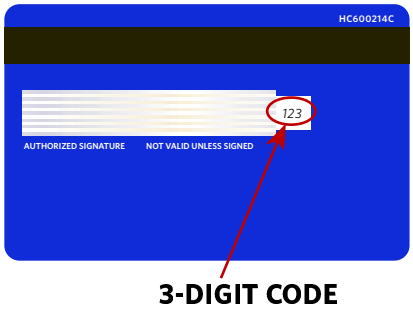
Safe Harbour – If a merchant has been deemed AIS compliant, they will be granted a "Safe Harbour" from any penalties/fees/fines by Visa Canada in the event of a hack or compromise. This applies to merchants who have validated their AIS compliance per the implementation framework, and are deemed AIS compliant after the post forensic investigation (by a Visa approved Qualified Incident Response Assessor).

3-Digit Code

What is the 3-Digit Code?

The three-digit security number (aka CVV2) imprinted on the signature panel of *Visa*® cards helps validate that the customer has a genuine card in his/her possession during an Internet or Telephone Order transaction (card-not-present transaction). The 3-Digit Code is required on all *Visa* cards, and is printed on the upper right portion of the signature panel of the card following the last four digits of the Primary Account Number (the entire Primary Account Number may or may not appear on the signature panel).

The 3-Digit Code provides a cryptographic check of the information embossed on the card.



Card Issuers may begin using this design after 2005.

3-DIGIT CODE

Please note: The entire Primary Account Number may or may not appear on the signature panel.

This card design will be discontinued by 2010.

3-DIGIT CODE

What is the process for the merchant?

After obtaining the card type, account number, and card expiration date, use the 3-Digit Code to verify the authenticity of the card:

- Ask the cardholder for the last three numbers on the signature panel of the card.
- Send the applicable presence indicator value with the authorization request:
  - **"0"** – 3-Digit Code value not provided (the merchant is not providing a 3-Digit Code value for verification).
  - **"1"** – The merchant is providing the 3-Digit Code value for verification.
  - **"2"** – The merchant wants to provide the 3-Digit Code value, but cannot because the cardholder states that the value is illegible.
  - **"9"** – The merchant wants to provide the 3- Digit Code value, but cannot because the cardholder states there is no value on the card.

3-Digit Code *cont'd*

Take the appropriate action when the 3-Digit Code response is received:

- **"M" (3-Digit Code matched)** – Indicates that Visa or the Issuer was able to verify the 3-Digit Code value provided by the merchant. Complete the transaction if the authorization request was approved.
- **"N" (3-Digit Code did not match)** – Indicates that Visa or the Issuer was not able to verify the CVV2 value provided by the merchant. Contact the cardholder to verify the 3-Digit Code before completing the transaction, even if the authorization request was approved.
- **"P" (3-Digit Code request not processed)** – Indicates that Visa or the Issuer was unable to verify the 3-Digit Code value provided by the merchant because their verification system was not functioning or not all the information needed to verify the 3-Digit Code value (such as the expiration date) was included in the request.
- **"S" (3-Digit Code should be on the card)** – Indicates that Visa or the Issuer was unable to perform 3-Digit Code verification, and notifies the merchant that the card should contain a 3-Digit Code value. Contact the cardholder to verify the 3-Digit Code before completing the transaction.
- **"U" (Issuer does not participate in 3-Digit Code service or has not provided Visa with encryption keys, or both)** – Indicates that the Issuer is not participating in the 3-Digit Code service, or has not provided Visa with encryption keys needed to perform verification.

Regardless of the 3-Digit Code verification response, if the Issuer does not approve the authorization request, do not complete the transaction.

How is the 3-Digit Code beneficial in a card-not-present environment?

The 3-Digit Code enables e-commerce (Internet) and Telephone Order merchants to ask for a unique 3-digit number on the back of *Visa* cards. Visa and the Issuers provide a real-time check of the code to help merchants verify that the person making the purchase physically has the card. If a purchaser only has the 16-digit credit card number and the expiry date, they may not have the card, signaling a potentially fraudulent transaction.

Other Information:

For information security purposes, all merchants are prohibited from storing the 3-Digit Code data.

Chargebacks for transactions with an unsupported 3-Digit Code response in the authorization response from Issuer:

If the merchant requests a 3-Digit Code response during authorization and received a "U" response from a Visa Issuer, it means the Issuer does not support the 3-Digit Code. In this situation, the Acquirer has the right to represent a fraud chargeback for that transaction on the merchant's behalf, **effective April 2005**.

Please note: the 3-Digit Code is being used by Canadian merchants more frequently. For more information, speak to your merchant services provider.

More information is available at *www.visa.ca/securewithvisa*.

Address Verification Service (AVS)

What is AVS?

The Address Verification Service (AVS) provides Acquirers that process mail order, telephone order or e-commerce transactions with a method of verifying the cardholder's billing address.

An address verification request includes the billing postal code and/or street address. It can be transmitted as a part of an authorization request, or as a separate request. The service verifies the address information and provides a result code to the merchant that is separate from the authorization response code. The merchant can then make an informed decision to continue with the transaction.

What is the process for the merchant?

- Ask the cardholder for the billing address, as it appears on their billing statement.
- Send the billing address with the authorization request.
- Visa® will provide one of the following AVS result codes with the authorization response:
  - **"A"** – Street addresses match. The street addresses match; the postal codes do not match or request does not include the postal code.
  - **"B"** – Street addresses match. Postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)
  - **"C"** – Street address and postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)
  - **"D"** – Street address and postal code match.
  - **"G"** – Address information not verified for international transaction.
  - **"I"** – Address information not verified.
  - **"M"** – Street address and postal code match.
  - **"N"** – No match. Acquirer sent postal code only, or street address only, or both postal code and street address.
  - **"P"** – Postal codes match. Street address not verified due to incompatible formats. (Acquirer sent both street address and postal code.)
  - **"R"** – Retry – The system is unavailable or timed out.
  - **"U"** – Address information not verified for that account number, or the card Issuer does not support AVS.
  - **"Y"** – Street address and postal code match.
  - **"Z"** – Postal code matches. Street address does not match or street address not included in request.

Regardless of the AVS result, if the Issuer does not approve the authorization request, do not complete the transaction.

Address Verification Service (AVS) *cont'd*

- Review all AVS failures. The address may be suspicious. Contact the cardholder to verify the address, and submit another AVS request.
- Research all partial AVS matches. A partial match indicates that compared addresses have the same postal code or address, but not both. Prior to completing the transaction:
  - Evaluate the historical risk associated with partial matches.
  - Contact the Issuer to verify that the name, address, and telephone number provided by the cardholder matches those on file with the Issuer.
- Evaluate all no-matches carefully. A no-match may indicate fraud, however, a no-match may be legitimate if the cardholder recently moved and did not update his new address with the Issuer. To evaluate a no-match, do the following:
  - Call the cardholder to verify that the telephone number belongs to the person who made the transaction, the address provided is correct, and to determine whether the cardholder recently moved.
  - Contact the Issuer to determine whether the name, address, and telephone number provided by the cardholder matches those on file with the Issuer.
  - Evaluate fraud rates by AVS result and product type.

How is AVS beneficial in a card-not-present environment?

AVS verifies cardholder information, and allows the merchant to send an address verification request to the card Issuer. Issuers compare the cardholder's billing address and postal code with the master file.

Other Information:

If the merchant requests an AVS response during authorization and receives a "U" response from a Visa® Issuer, it means the Issuer does not support AVS. In this situation, the Acquirer has the right to re-present a fraud chargeback for that transaction on the merchant's behalf, **effective October 2006**.