TD Canada Trust

How to Help Prevent Fraud

Merchant Services tips to help protect your business

Fraud Awareness

All credit cards issued in Canada are designed with special security features to help deter counterfeiting and fraud. A fraudulent credit card transaction could involve an invalid account number, or the unauthorized use of a valid account number.

One of the common types of fraud loss is due to unauthorized use of a lost or stolen credit card. Fraudulent transactions normally occur within hours of loss or theft. In most cases, the victim has not yet reported his/her card as missing or stolen.

Procedures have been established by the Payment Card Networks to help you detect fraudulent cards and take appropriate action when necessary. In addition, card security features have been designed to facilitate the detection process.

The information in this brochure is provided to help you protect your business against fraud losses.

New technology helps you reduce fraud

TD Merchant Services is working to provide additional credit and debit card fraud awareness and prevention techniques. These include CHIP technology, where a microcomputer chip is embedded in credit and debit cards, allowing merchants to process transactions more securely and conveniently.

Debit and Credit Card Fraud Awareness

While CHIP transactions are among the most secure in the world, debit and credit card fraud resulting from skimming can occur. Skimming refers to the fraudulent practice of capturing account information from the magnetic stripe of a debit or credit card in order to make a counterfeit card.

Personal Identification Numbers (PINs) may also be stolen.

Here are the steps you can take to help prevent skimming:

- Inspect your POS equipment regularly – including serial numbers, wires and cables. If any equipment looks unfamiliar, appears altered, or is missing, notify TD Merchant Services immediately.
- Check ceilings, walls or shelves near PIN pads for holes that could conceal a small camera.
- Install your debit terminal so that customers have enough room to comfortably shield the PIN pad when entering their PIN number. The most common way of stealing a cardholder's PIN is by "shoulder surfing" – looking over the cardholder's shoulder.
- Make sure that any security cameras on your premises don't capture customers entering a PIN.
- Never enter a PIN for a customer, even if asked to do so.
- Remember to give the customer a copy of the transaction receipt.

- Allow the customer to hold the PIN pad until the transaction is complete.
- Keep all transaction records on file (for the length of time specified in your processing service agreement), along with employee shift schedules and supplier information.

Credit Card Fraud Prevention Checklist

The risk of allowing unauthorized fraudulent credit card transactions is reduced if you follow the proper procedures on every credit card transaction, including:

1. Check that the credit card presented bears all of the usual symbols and marks:

☑ The four-digit printed number above or below the account number displayed on the front of the card.

☑ The three-dimensional hologram on the front of the card or the mini hologram or holographic magnetic stripe on the back of the card.

Please see pages 7-10 for additional details

2. Ensure that the imprint is clear and legible on all copies of any sales drafts:

☑ If you have an electronic terminal and cannot swipe the card through your terminal, you may key the transaction manually. Take special care to review the security features of cards that do not swipe successfully.

☑ Also, you must ensure you take a manual imprint of the credit card as proof that the card was present during the transaction. Make sure you have a merchant plate affixed to the manual imprinter. Record the date, authorization number and amount on the imprinted sales draft and ensure that the customer's signature is obtained on the imprinted sales draft. If you are experiencing persistent problems in processing your customers' cards through your terminal, please contact TD Merchant Services for assistance.

3. Call for an authorization if:

☑ Your electronic terminal gives you the message "Call for Auth."

☑ The account number that appears on your terminal screen does not match the account number displayed on the front of the card.

☑ You are suspicious of the cardholder, credit card or signature.

Be aware that obtaining an authorization number only confirms the funds are available on the card. It does not confirm that the cardholder authorized the transaction nor does it prevent a chargeback.

NOTE: If you are using an electronic terminal, your floor limit will be provided to you by TD Merchant Services. If your terminal is not working due to power failure or system problems, please revert to your manual floor limit procedures, i.e. phone for authorization, record the authorization number on the sales draft and take a manual imprint of the credit card on any transactions equal to, or greater than, your manual floor limit.

4. Ensure that the cardholder's signature on the sales draft matches the one on the signature panel of the credit card. Ask for identification if necessary.

CODE 10 authorization

Whenever you are suspicious of a credit card transaction or a cardholder, call the TD Merchant Services Authorization Centre immediately at **1-800-363-1163** and identify your call as a CODE 10 authorization.

The CODE 10 authorization is a procedure designed to alert the operator that you suspect that the transaction may be fraudulent or suspicious, without alarming the individual who is presenting the card. A series of "yes" or "no" questions will be asked to verify the authenticity of the card. The operator may give you an authorization code or may instruct you to retain the credit card. It is for this reason that you should hold the card throughout the authorization process.

Do not try to apprehend or detain the person using the credit card. Take note of his or her physical appearance and of any other relevant information, in case the person leaves your premises.

Security features of all credit card designs

Recognizing suspicious cards is a good first step toward protecting yourself against credit card fraud. You need to know what security features appear on each type of card, and you should be able to recognize common signs of tampering in order to detect cards that may be fraudulent or counterfeit.

Before accepting a card, make sure the account number shows no signs of re-embossing or alteration. Check that the validity dates, which are embossed below the account number, do not appear altered. Do not accept a card that is being used prior to the "Valid from" date or after the "Good thru" date.

All cards have a signature panel on the back. Compare the signature on the signature panel with the one on the sales draft for correct spelling and similar handwriting. If they are different, do not hesitate to ask for identification. Never accept an unsigned credit card.

You should check the signature panel for obvious signs of tampering, such as scratching, the presence of white tape or white correction fluid, or signs that a felt-tipped pen has been used to write over a pre-existing signature. If you can see the word "void" repeated on the signature panel, then the panel has been erased or compromised in some way and you should not accept the card.

All cards have a magnetic stripe on the back which is encoded with account information. This stripe should be smooth and straight and show no signs of tampering.

If you have an electronic terminal, the magnetic stripe is read and the account number is displayed on your terminal screen each time you swipe a card. Make sure the number that appears on the screen matches the account number on the front of the card. When the receipt is printed, you should also compare the account number on the receipt with the one on the card. Only on a swiped transaction, if the numbers do not match, call for a CODE 10 authorization.

On the following pages, you will find images of the front and back of *Visa** and *MasterCard*® designs, along with a guide to the specific security features of each one. Familiarize yourself with these features so that you will be able to recognize suspicious cards and protect yourself against fraud.

EMV liability shift

Did you know that if you process an EMV CHIP card by using the magnetic swipe you could be found liable for a chargeback, unless your terminal prompted you to do so.

Security Features

Visa Card

1 The Account Number

All *Visa* account numbers have 16 digits and begin with a 4. You should check that the numbers are clean and clear, and that all the numbers are the same size and regularly spaced. If the numbers appear fuzzy, the card may have been re-embossed.

2 Bank Identification Number

The first four digits of the account number are the Bank Identification Number (BIN) and are repeated below the embossed numbers in smaller type. You should check that the four numbers below match the first four embossed numbers above. If they do not, the card has been modified or is counterfeit.

3 *Visa* Brand Mark

The *Visa* Brand Mark appears in the bottom right corner or the top right or left corner of the card. It is horizontal on most cards, though it may be vertical on CHIP cards.

If you place the card under an ultraviolet light, you should be able to see a letter "V" over the *Visa* Brand Mark.

4 CHIP

An embedded microchip that stores information in a secure, encrypted format makes it more difficult for unauthorized users to copy or access the information on the card.

5 *Visa payWave*®

(Optional) *Visa payWave*® contactless payment technology may be present on a card. A signature is not required for *Visa PayWave*® "tapped" transactions.

6 Signature Panel

The signature panel, which may look like this or be custom designed, must appear on the back of the

TD Business *Visa Card without CHIP**

TD® Aeroplan® *Visa Infinite*² Card with CHIP

card. If you put the card under an ultraviolet light, you should see the word "VISA" repeated on the panel.

7 Mini Dove Hologram

The mini dove hologram appears on the back of the card, either below or to the left or right of the signature panel on non-CHIP cards, and below the signature panel on CHIP cards.

8 Magnetic Stripe

Make sure the magnetic stripe is smooth and straight, and does not show any signs of tampering.

9 Card Verification Value 2 (CVV2)

Check for the three-digit CVV2 code, which will be reverse indent-printed either on the signature panel itself or in a white box to the right of the signature panel.

MasterCard Card

1 Account Number – First 4 Digits

The first four digits of the account number must match the four-digit preprinted BIN. Remember, all *MasterCard* numbers start with the number 5.

2 Account Number – Last 4 Digits

The last four digits of the account number must match the four digits that appear on the cardholder receipt.

3 Global Hologram

The global hologram is three-dimensional with a repeat *"MasterCard"* printed in the background. When rotated, the hologram will reflect light and appear to move.

4 Signature Panel

The signature panel is tamper evident with the word *"MasterCard"* printed in multiple colours at a 45-degree angle. For magnetic swiped transactions, remember to compare the signature on the back of the card with the cardholder's on the receipt.

5 Card Verification Code 2 (CVC2)

The four digits printed on the signature panel must match the last four digits of the account number, followed by the three-digit indent-printed CVC2 number.

6 CHIP

An embedded microchip that stores information in a secure, encrypted format, makes it more difficult for unauthorized users to copy or access the information on the card. The cardholder will be prompted to enter a unique personal identification number or PIN when the card is inserted into a CHIP-capable payment terminal.

7 *PayPass*™

(Optional) *PayPass* contactless payment technology may be present on a card. A signature is not required for *PayPass* "tapped" transactions below a specific limit.

Watch for suspicious behaviour…

While any of the following can occur in a perfectly legitimate transaction, some or all of these characteristics are also frequently present during fraudulent transactions. Be alert for the customer who:

- Makes random purchases with little regard for price, size, colour or style.
- Purchases an unusual quantity of expensive items.
- Charges expensive items on a newly valid credit or debit card.
- Purchases large items such as TVs or stereos, and insists on taking the merchandise immediately even when delivery is included in the price.
- Makes several small purchases in order to test the card's acceptance.
- Removes the credit or debit card from a pocket rather than a wallet.
- Provides multiple cards to make a single purchase after a decline (especially in a card-not-present transaction or a transaction with magnetic swipe cards).
- Cannot provide photo identification upon request.
- Hurries the clerk at quitting time or is excessively talkative because of nervousness or in an attempt to frustrate the clerk.
- Seems too familiar with your terminal's functionality or provides you instructions on how to process the card.
- Overpays for your services and requests a wire transfer, money order or certified cheque.

Card-not-present fraud

What is card-not-present fraud?

Card-not-present fraud refers to fraudulent transactions that occur without the use of an actual card. Typically, it occurs in situations where customers provide only a credit card number, such as in online, telephone or mail-order transactions. Because the card is never presented to you, you have no way of checking its validity using the security features outlined on pages 7–10.

Card-not-present fraud is the fastest-growing type of fraud in Canada. It is popular with criminals because it allows them to commit fraud without the risks involved in going into a store and attempting to make a purchase with a counterfeit or altered card.

What are *Visa* and *MasterCard* doing to help prevent card-not-present fraud?

To help you protect yourself from card-not-present fraud, *Visa* has developed the *Verified by Visa** program, the Address Verification Service (AVS) and added the Card Verification Value 2 (CVV2) to all cards. *MasterCard* has developed the *MasterCard SecureCode*® program and the Address Verification Service (AVS) and added the Card Verification Code 2 (CVC2) to all cards.

What are the *Verified by Visa* and *SecureCode* programs?

Verified by Visa and *MasterCard SecureCode*®[1] use a password system to add a new level of security to online *Visa* card and *MasterCard* card transactions. A cardholder creates a password, which they enter whenever they make a purchase at the website of a merchant who participates in *Verified by Visa* and *SecureCode*. This helps ensure that the person making the purchase is the actual cardholder and not just someone who has the account number of a card.

Your customers are aware of the growth in online credit card fraud and, when they see that your website participates in *Verified by Visa* and *SecureCode*, it can help make them feel secure about purchasing through your website. As well, if you participate in the *Verified by Visa* or *SecureCode* programs, you can receive greater protection from fraud-related chargebacks.

What are the Card Verification Value 2 (CVV2) and Card Verification Code 2 (CVC2)?

CVV2 and CVC2 are credit card security features that help you ensure that the person making an online, telephone or mail-order purchase from you is actually a legitimate cardholder. The CVV2 and CVC2 are three-digit security codes that appear on or to the right of the signature panel on the back of *Visa* and *MasterCard* cards. (See the card visuals on pages 8 and 10 for examples of the CVV2 and CVC2.)

How do the CVV2 and CVC2 protect you against fraud?

Whenever you take a card-not-present order – online, by phone or by mail – make sure you request this three-digit number. The *Visa* and *MasterCard* systems provide a real-time check to ensure that the CVV2 or CVC2 you have been given is the one properly associated with the account number provided by the customer.

By supplying the CVV2 or CVC2, the customer shows that they are actually in possession of the card. If the customer has only the account number or the account number and expiry date, it may indicate that the transaction is fraudulent.

What is the 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 decide whether to continue with the transaction based on the results code. Issuers are 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.

Hacking

As businesses come to depend more and more on technology, criminals look for new ways to exploit technology for their own purposes. Today's tech-savvy criminals can hack into your computer system to gain access to sensitive information about you, your business and your customers.

How does *Visa* and *MasterCard* help protect your business against hackers?

The *Visa* Account Information Security (AIS) and *MasterCard* Site Data Protection (SDP) programs are global programs that help make both the virtual and the physical portions of your business more secure. AIS and SDP provide you with an easy-to-use toolkit designed to help you protect cardholder account and transaction data against unauthorized access by hackers. The AIS and SDP programs incorporate a self-assessment questionnaire that lets you evaluate how well your business is protected.

What else are *Visa* and *MasterCard* doing?

Visa and *MasterCard* have aligned with a data security standards program offered by other payment organizations to create a Payment Card Industry (PCI) set of data security standards. This alignment of standards is designed to increase the security of card information and further protect cardholders and merchants against fraud. It also simplifies things for merchants like you, by establishing one set of security standards for you to implement.

How can *Visa* and *MasterCard* help ensure your business is secure?

To assess how secure your business is against fraud, you can visit **visa.ca/securewithvisa** Additionally, visit **visa.ca/ais** and **mastercard.com/ca/merchant** to confirm your business complies with the Payment Card Industry Data Security Standards (PCI DSS). For more information on the PCI Council, visit **pcisecuritystandards.org**

What steps can you take to protect your business?

There are a number of procedures you can follow to help keep your business safe from hackers. Protect your systems and data against viruses with security software, and make sure you keep the software up-to-date. Any data that is sent across networks or stored on Internet-accessible databases or files must be encrypted, and you should never continue to store data that is no longer needed for business purposes. When you are done with the data, destroy it in a secure fashion so that it is not accessible to anyone hacking into your system. If at any time you believe that account or transaction information has been stolen, report it immediately to TD Merchant Services.

Remember that criminals commonly use phone calls to fraudulently extract information from businesses. Make it a policy never to give account data over the phone unless you made the call yourself.

How can you safeguard your customers' information?

Any documents containing credit card account numbers should be stored and destroyed in a secure manner to safeguard your customers' information.

Are there specific steps you should take with regard to your employees?

Your business is only as secure as your employees make it. To help protect account data, give your employees access to it only on a need-to-know basis. Whenever an employee leaves, immediately revoke their access to your network and your premises.

To help your employees protect your business against fraud, train them in how to recognize suspicious practices and establish a system that lets them report these occurrences to you.

With these standards and practices in place, you should have a more secure business that protects both you and your customers against fraud.

For your own protection

Beware of sales draft laundering or factoring. Typically, this is a scheme where, in return for processing a third party's sales drafts through your merchant account, you are offered a generous commission or fee. This practice is in violation of your Merchant Services Agreement with us and can result in chargebacks and the immediate termination of your Merchant Services Agreement. If the drafts turn out to be fraudulent, you may be charged with a criminal offense. Do not be tempted to process drafts belonging to another business or party. It's not worth the risk!

Please immediately report any suspicious activity involving credit card or debit card use to TD Merchant Services at
1-800-363-1163

For more information, visit
tdmerchantservices.com

581614(1113)