

# Contact

Business-building ideas for TD Merchant Services customers

**SPECIAL FRAUD PREVENTION ISSUE**

## 5 ways to safeguard your business

In 2003, credit card fraud cost Canadian cardholders and merchants more than \$138 million. What can you do to fight back? Here are some best-practice suggestions to help you protect your customers and your business.

### 1. Check every card

When you are presented with a *Visa* \* card, make sure it bears all of the standard *Visa* symbols and marks (see details on Page 2). These include the three-dimensional dove hologram, the printed number above or below the embossed number (which should match the first four numbers of the embossing), and a signature panel that bears the repeated word “*Visa*” in blue and gold. Also check the expiration date, and make sure the last four numbers of the card are embossed in the hologram.



BUSINESS BOOSTERS

### 2. Swipe the stripe

The magnetic stripe is a key component of a credit card’s security, so it’s important to swipe each card through a point-of-sale (POS) terminal whenever

possible. Swipe the card once in the direction of the arrow shown on the reader, then check that the account number displayed on the terminal screen matches the one on the card.

If the card won’t swipe, get a manual imprint of the card and follow procedures for key-entered transactions.

### 3. Follow processing procedures

If authorization is required, obtain an authorization number before processing the transaction. Do not give the card back to the customer until the authorization is complete.

### In this issue

#### 2 / Business boosters

- Fraud-fighting features

#### 3 / Managing your business

- Preventing card skimming
- Beware of bogus international orders

#### 4 / Fraud prevention

- Card fraud: What to watch for
- How Code 10 works



Continued on Page 2

## 5 ways to safeguard your business

*Continued from Page 1*

Ensure that the sales draft is signed (and imprinted in the case of manual transactions) and that the signature matches the one on the card. Never accept an unsigned card.

### 4. Be vigilant with off-site orders

The risk of fraud is even greater during mail, telephone, fax or Internet transactions where the card itself is not present. Transactions completed in this way do not permit normal cardholder identification and, in the event of fraud, could result in a chargeback and loss of the entire transaction amount. (Please note that you must be approved by TD Merchant Services to accept *Visa* card payment orders by mail, telephone, fax or Internet.) To reduce the risk of becoming a victim of fraud, use the following security procedures before calling for authorization:

- If delivery and billing addresses differ, ask the customer for day and evening telephone numbers. Verify these through directory assistance or by visiting [www.canada411.ca](http://www.canada411.ca) and call back to validate the order.
- If the order is to be picked up, ask the customer to bring his or her *Visa* card and take the opportunity to swipe it (or get a manual imprint) and obtain the customer's signature on the receipt.
- Ask for the card expiration date and the Card Verification Value 2 (CVV2). The CVV2 is a three-digit number imprinted after the account number on the signature panel of *Visa* cards. These numbers are used to help merchants validate that the customer has a genuine card in hand during a mail, telephone, fax or Internet transaction. The CVV2 was developed

as a way to minimize fraud; however, it does not guarantee that the actual cardholder completed the transaction.

- For Internet orders, consider additional security with *Verified by Visa*,\* an online payment feature that helps authenticate cardholder identity with the use of a password. To find out more about the program, visit [www.visa.ca/verified](http://www.visa.ca/verified)
- Apply good business judgment. Does the transaction make sense in the context of your business? Does the reward of completing this transaction outweigh the risk of completing it?

### 5. Take the time to train your staff

It's important to educate your front-line employees about proper card processing and Code 10 procedures. Explain when to be wary in certain sales situations (see details on Page 4). TD Merchant Services can provide you with written material to help you teach your staff about fraud prevention.

For more information on how you can help protect your business from fraud, call the TD Merchant Services Help Desk at 1-800-363-1163 and ask for a copy of our credit card fraud prevention brochure. ■

## Fraud-fighting features

*Visa* cards have a number of built-in security features designed to help you recognize a real card from a counterfeit one. Here's what to look for:

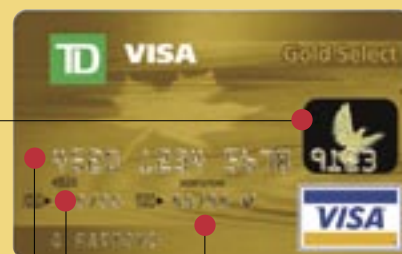
**Dove hologram:** Does it look three-dimensional and do the dove's wings appear to move as you tilt the card back and forth? Are the last four digits of the account number embossed in the hologram?

**Embossing:** Is it clear and straight? Does the 16-digit account number begin with the number "4"?

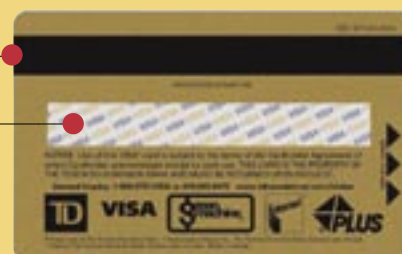
**Four printed numbers:** Do they match the first four numbers of the embossing?

**Magnetic stripe:** It contains coded account and other information. Check that the magnetic stripe is a permanent part of the card and shows no signs of tampering.

**Signature panel:** Does it bear the repeated word "*Visa*" in blue and gold at an angle? Compare the signature on the back of the card with the signature on the sales draft for correct spelling and similar handwriting. If they are different, ask for identification. Do not accept an unsigned *Visa* card.



**Expiration date:** Do not accept a card that is being used prior to the "valid from" date and do not accept an expired card.



**If, for any reason, you suspect fraud, make a Code 10 call (see Page 4).**

# How to prevent card skimming

**S**kimming refers to the capture of account information from the magnetic stripe of a debit or credit card for the purpose of making a counterfeit copy.

As a result of the increasingly sophisticated technology available today, it is now easier than ever for criminals to “skim” information from cards using either an altered or dummy terminal. Here are some tips on how to stop skimming.

## Know your equipment

Do a regular inspection of your POS terminals and PIN pads, and periodically check serial numbers. If the number of devices, or their appearance, changes, report it to TD Merchant Services immediately.

Also check the POS area and under counters for any equipment, wires or cables that don't belong. Watch for unfamiliar devices, no matter how small. The newest high-tech skimmers are about the size of a pager and can be clipped to a belt or kept in a pocket.

Look for areas above PIN pads where a small camera may be placed to record customers entering their PIN (such as suspicious holes in the ceiling or walls, or on an upper shelf).

## Know your operation

Businesses with staff working alone for long periods of time, at night or on weekends, are particularly vulnerable to skimming. Consider making random “spot check” visits during these hours.

Also establish clear record-keeping policies and procedures. Keep accurate employee shift schedules on file for 12 months, so you can always tell who had access to the POS terminal and when.

Keep a record of suppliers (such as

cleaners, electricians, painters) that work for you, especially after hours. Check that these companies keep the names and verified contact information of their employees on file.

## Know your staff

It's important to practise due diligence when hiring and supervising employees:

- Before hiring, check government-issued photo identification and references.
- Obtain and record a new employee's full name, address, telephone number, date of birth and Social Insurance Number.
- Require employees to sign or write



their employee number on each transaction draft, and monitor this process from time to time.

- Consider offering a reward to employees who report skimming activity or who report being approached by skimming groups. ■



## Beware of bogus international orders

In recent months, there has been a dramatic rise in the number of fraudulent orders placed to Canadian businesses from overseas.

Typically, a merchant will receive a small initial order from an overseas customer by phone or email that establishes the relationship.

A second order may follow requesting a much larger shipment of merchandise to an international address.

Be cautious if this situation arises, or if any international order involves the following:

- Orders shipped to a single address but split between several credit card numbers.
- A shipping address that is different from the cardholder address, especially where the countries differ (for example, the order is on an Australian card, but the goods are to be shipped to Bulgaria).
- Unusually large quantities, high-value items or multiples of the same item – especially if they are to be shipped rush or overnight.
- Requests for products that your business usually doesn't sell.

If you are suspicious of an overseas order, follow the guidelines recommended for processing card-not-present transactions (see Page 2) – including verifying the card's CVV2 security code – and follow proper authorization procedures.

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

# Card fraud: What to watch for

Identifying the early warning signs of a potentially fraudulent transaction can save your business time and money. Both credit cards and customers can exhibit suspect characteristics that can warn you of potential problems.

Examine credit cards carefully to detect signs of tampering or counterfeiting, and keep a close eye on the behaviour of unfamiliar individuals in your place of business.

## Problems with the card

- A bumpy, chipped or scratched surface with bent edges.
- A missing three-dimensional hologram.
- Metallic paint used to touch up the hologram after re-embossing the account number.
- A mismatch between the printed four-digit number and the first four embossed numbers.
- Irregular or inconsistent spacing and type styles.
- A signature panel that's been painted, taped over, damaged or erased, exposing the word "VOID."

- Ghost images of a previous name, number or date.

## Problems with the "customer"

- Customers who purchase large quantities of high-priced merchandise on a newly valid card without regard to size, colour, style or price.
- A female customer using a card with a male name, or vice versa.
- Someone who purchases expensive electronics such as TVs or stereos without asking about technical specifications or warranties, or insists on taking merchandise immediately, even when delivery is included in the price.
- Customers who take their credit card from a pocket rather than a wallet, who sign the sales draft very slowly or awkwardly or need to see the name on the card before signing.
- A customer who appears extremely nervous or is hurrying the clerk at closing time.

Although these situations can be present in a legitimate transaction, it's best to play it safe. If you have any suspicions, call for a Code 10 authorization. ■

## How Code 10 works

If your experience, instincts, or any of the information in this newsletter lead you to suspect a credit card might be fraudulent, call the TD Merchant Services Visa Authorization Centre immediately (1-800-363-1163).

Identify the call as a Code 10 authorization and proceed as follows:

- Stay calm and courteous and hold on to the card until you have obtained authorization.
- Respond to the authorizer's questions with appropriate "yes" or "no" answers.
- Follow instructions to either complete the transaction (with the authorization number provided) or retain the card.
- Do not try to apprehend or detain the cardholder.

While it is important to report suspected fraudulent transactions, reporting a Code 10 should never be done at the risk of one's own personal safety.

## Time to order paper?

The following companies are preferred suppliers of paper for TD Merchant Services point-of-sale terminals. To ensure you are

dealing with a reputable dealer, give one of them a call when you need paper.

- J.L. Inc., 1-800-363-4873

- Main-Tech Industries, 1-800-268-5120
- Maxwell Media Products, 1-800-561-6406
- Wedge Paper Products, 1-888-933-4336

Contact is published periodically by TD Merchant Services. For more information, please write to: Contact Newsletter, TD Merchant Services Marketing Department, Royal Trust Tower, 15th Floor, Toronto, Ontario M5K 1A2; or call toll-free 1-800-363-1163; or visit [www.tdcanadatrust.com/merchantservices](http://www.tdcanadatrust.com/merchantservices)

♻️ Printed on recycled paper.

TD Merchant Services does not recommend, or offer any advice regarding the nature, suitability, or potential value of, any particular service or product.

Every effort has been made to ensure that the information contained in this newsletter is accurate. However, TD Merchant Services and The Toronto-Dominion Bank are not liable for any errors or omissions in the information or for any loss or damages suffered arising from such errors or omissions.

\* Visa International Service Association/TD Canada Trust licensed user of Mark.

© 2005 The Toronto-Dominion Bank, All Rights Reserved.

 **Merchant Services**