

Contact

Business-building ideas for TD Merchant Services customers

Top 5 reasons why data security matters

Canadians reportedly use credit cards almost as widely as cash.¹ And the more frequently cards are used, the more cardholder account information is being processed and potentially kept on file.

In the last issue of *Contact*, we explained how Visa Canada's Account Information Security (AIS) program helps you prevent the theft of that confidential account information.

The AIS program requires merchants to uphold and maintain the Payment Card Industry (PCI) Data Security Standard set by the payment industry worldwide (visit www.visa.ca/ais for a detailed list of these requirements and compliance information). Here are the key ways protecting data can benefit your business.

1. Build consumer trust

Many customers not only seek out merchants they feel they can trust, but are also likely to return to those businesses



and tell others. In a 2006 Visa-sponsored survey that spanned 12 countries, consumers ranked the security of personal

and financial information as their number-one concern. These consumers also indicated that merchant data security practices can influence their desire to purchase products and services.

Complying with industry standards helps demonstrate your commitment to protecting your customers' confidential payment information. This security is essential to building and maintaining consumer trust.

In this issue

2 / Business boosters

- Tips for safeguarding data

3 / Managing your business

- Chip card checkup
- New developments in the payment card industry

4 / Fraud prevention

- Fraud prevention checklist
- Get ready for MasterCard
- Need paper?

Continued on Page 2

Top 5 reasons why data security matters

Continued from Page 1

2. Strengthen security

The main goal of the AIS program and PCI Data Security Standard is to protect confidential data at all points in the payment system. Complying with the program improves awareness of data security and helps you strengthen security measures to minimize the possibility of data security attacks.

3. Avoid unnecessary costs

Implementing a strong data security policy will help you prevent a security

breach that could cost your business by damaging your reputation and your bottom line.

Data breaches resulting from weak security practices could make your business vulnerable to costly forensic review, litigation, penalties and an overall drain on your business operations.

By implementing effective data security standards, you can avoid these expenses and protect your business's good name.

4. Maintain a positive image

If you have made every effort to comply with the PCI Data Security Standard, this compliance will go a long way toward

protecting your reputation in the eyes of your customers and the press, given growing public concerns about safeguarding personal data.

5. Gain a competitive edge

A strong data security policy can help you build a reputation for trustworthiness and reliability. When your customers are confident their confidential account information is safe with you, their repeat business will boost your bottom line and give you an advantage over the competition.

For more information about how to keep your customers' account information more secure, visit www.visa.ca/ais

Tips for safeguarding data

Keeping your customer data safe from hackers makes good business sense. Here are some useful guidelines to help you protect your confidential customer information — and your business.

- Keep cardholder information storage to a minimum and never store the information contained in a credit or debit card's magnetic stripe.
- When you no longer need the account information, destroy it in a secure fashion. Never store the CVV, CVV2 or PIN.
- Be aware that some software programs may store data automatically. Review software and update preferences to be sure account information is not being stored behind the scenes.
- Comply with security audits according to the PCI requirements. (For details, see www.pcisecuritystandards.org)
- Use adequate firewalls.
- Change system passwords and security codes from those originally supplied by software manufacturers.
- Encrypt all payment card information stored on the processor's computers.
- Encrypt any card data transmitted over the Internet or other open public network.
- Use and regularly update your anti-virus software.
- Keep other software, such as operating systems, secure and updated.
- Only allow employees access to customer data on a need-to-know basis. As well, each employee with computer access should receive a unique ID.
- Restrict physical access to hard-copy payment card data.
- Test the company's security systems on a regular basis.
- Have an information security policy that spells out rules for employees who handle data. Reinforce it regularly.
- Require all third-party suppliers with access to cardholder data to adhere to payment card industry security requirements.



Chip card checkup

Members of Canada's payment industry — Visa Canada Corporation, MasterCard Canada, Inc. and Interac Association — are working together to introduce chip technology to the Canadian market over the next few years.

As part of this effort, in the fall of 2007, these associations launched a year-long chip technology market trial that introduced chip-enabled credit and debit cards to a test market of 200,000 Kitchener-Waterloo consumers. Local merchants also received 2,300 chip-enabled point-of-sale (POS) terminals, and 65% of ABMs were updated with chip card technology.

“Merchants and consumers have much to gain from the migration to chip technology,” says Tracey Black, trial program director. “Chip cards and chip terminals make a secure transaction system even more secure.”

Positive results. A recent survey of more than 200 merchants and front-line staff who participated in the market trial yielded positive results, namely:

- **Consistent PIN recall.** Most respondents found that 70% to 80% of customers remembered their PIN when completing a transaction using the chip credit card.
- **User-friendly screen prompts.** A majority of merchants and front-line staff surveyed found that terminal screen prompts directing cardholders through the transaction were easy to read and follow and resulted in little or no difficulty for most customers.
- **Increased security welcomed.** Positive comments from customers indicated that cardholders were generally pleased about the increased

security and safety of using a PIN (versus signature-only card).

- **Checkout time unaffected.** Up to 88% of those surveyed found checkout times using chip cards to be the same or less than with non-chip cards.

Reviewing payment procedures. Most retailers reported having limited experience with chip-and-PIN transactions, which require the card to be inserted into, and remain within, the terminal while a PIN is entered and the transaction completed.

With chip card transactions, the customer inserts the card into the terminal,

which displays the purchase amount and requests a PIN. Once the PIN is confirmed and the purchase approved, a receipt is printed. When the transaction is complete, a prompt appears on the screen to remove the card from the terminal.

“All chip cards will continue to have a magnetic stripe on the back,” explains Tracey Black, allowing merchants with magnetic-stripe-only POS terminals to accept payments as usual.

Watch for updates on our conversion to chip technology in future issues of this newsletter or by visiting www.tdmerchantservices.com ■

Making change: New developments in the payment card industry

The new chip card (see story above) is just one of several security-boosting developments taking place within the payment card processing industry. Here is a sneak preview of two others.

Contactless cards

New contactless cards — such as the *Visa payWave** card — combine the security benefits of chip technology with a convenient no-swipe, no-PIN checkout. These cards are proving ideal for low-value, quick-service transactions, such as coffee shops, movie theatres and newsstands.

The cardholder simply waves the card — which is embedded with an antenna and a microchip — in front of a contactless reader for a secure, fast way to pay.

PCI DSS upgrade

In October, the PCI Security Standards Council will release Version 1.2 of the PCI Data Security Standard (DSS) (see Page 1 story). The existing 12 core requirements of the PCI DSS will remain the same; however, this updated version will clarify these requirements and make the standard easier to understand and implement. Version 1.2 will:

- Explain PCI DSS technical requirements in more detail.
- Provide clarification on how to submit security reports.
- Incorporate new best-practice recommendations.
- Include a section explaining the security process through FAQs and a glossary.

Fraud prevention checklist

With the hectic holiday season fast approaching, it is an ideal time to review fraud-prevention procedures with front-line staff. Here are some suggestions to help protect your business from fraud during this busy period.

Best-practice procedures

When processing credit card transactions, always follow proper authorization procedures and check the following security features:

- Transaction receipt and back-of-card signatures should match.
- Four-digit number that appears under the embossed number needs to match first four embossed numbers.
- Dove hologram must be 3-D, not a flat image.
- Expiration date should still be valid.

For manually keyed transactions, verify that you get a clear, legible imprint of the customer's *Visa* card on all copies of the sales draft. If you have an electronic terminal and cannot swipe the card through the terminal, key in the transaction manually. Take a manual imprint and make sure you have a merchant plate affixed to the imprinter. Also, ensure that all pertinent information — such as customer signature, date, authorization number and amount — is filled out on the manual imprint in case of dispute.

Fraud trends

TD Merchant Services fraud experts report a rise in fraud involving telephone,

mail order and Internet transactions, and recommend using caution when the card itself is not present.

- 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 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.
- 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

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.

Signs to watch for

Here are some out-of-the-ordinary shopping behaviours to watch for:

- Unusually large purchase totals (especially if ordered sight-unseen by phone, fax or Internet).
- Purchases of several varieties of the same "big ticket" item, especially if charged to a newly valid credit card.



- A customer insisting on taking high-value merchandise (such as a TV or stereo) immediately, even when delivery is included in the price.

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

Get ready for MasterCard

We can help you get ready to accept MasterCard® from your customers. To get started, please contact First Data by telephone at 1-866-306-7874 or email merchantservicescanada@firstdata.com

Need paper?

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

- MainTech Industries, 1-800-268-5120
- Maxwell Media Products, 1-800-561-6406
- Papier Parfait Inc., 1-877-745-5163

Contact is published periodically by TD Merchant Services. Every effort has been made to ensure that the information contained in this newsletter is accurate. However, TD Merchant Services is not liable for any errors or omissions in the information or for any loss or damages suffered arising from such errors or omissions.

For more information, please write to: Contact Newsletter, TD Merchant Services Marketing Department, 100 Wellington St. W.,

29th Floor, Canadian Pacific Tower, Toronto, Ontario M5K 1A2; or call toll-free 1-800-363-1163; or visit www.tdmerchantservices.com

1. Interac Association 2007.



Mixed Sources
Cert no. SW-COC-001700
© 1996 FSC

* Visa International Service Association/Used under license.
® Registered trade-mark of MasterCard International Incorporated.
© 2008 The Toronto-Dominion Bank. All Rights Reserved.

TD Merchant Services