

Contact

Business-building ideas for TD Merchant Services customers

SPECIAL FRAUD AWARENESS ISSUE

Working together to keep customer data secure

Today's tech-savvy criminals are hard at work trying to find new ways to hack into business computer systems and gain access to confidential customer account information that they can use to commit fraud. To beat them and protect our businesses, we need to work even harder.

Visa Canada's Account Information Security (AIS) program is a key weapon for you to use in this fight. It is designed to help merchants prevent the theft of cardholder data by assessing whether cardholder data is secure within your organization and, if necessary, improving your level of security to meet or exceed industry standards.

How AIS works

The AIS program requires that merchants: (i) comply with the Payment Card Industry (PCI) Data Security Standard



– a set of requirements that are followed worldwide by all the major credit card associations and issuers; and (ii) validate that compliance. All merchants who process, transmit, store or access Visa* credit card information must comply with AIS. Whether your customer credit card information resides on a stand-alone PC or on a network server, the AIS program works to protect confidential data at all points in the payment system.

Key requirements

In order for merchants to comply with the AIS program, they must meet the following 12 basic requirements of the

PCI Data Security Standard (plus more detailed sub-requirements):

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

Continued on Page 2

In this issue

2 / Business boosters

- Privacy matters

3 / Managing your business

- Visit our new website
- Chip card update

4 / Fraud prevention

- Protect your PIN pads

Working together to keep customer data secure

Continued from Page 1

7. Restrict access to sensitive cardholder data on a business need-to-know basis.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

How to be validated

Each merchant falls under one of five validation levels, based on the annual volume of *Visa* transactions processed. This level determines the activities that the merchant needs to follow in order to be validated under the AIS program.

- Although recommended for all merchants, AIS validation is mandatory for all merchants who fall under any of the first four validation levels (i.e. any merchant processing more than 20,000 *Visa* e-commerce transactions per year, and all other merchants processing more than one million *Visa* transactions per year). These merchants are required to:
1. Enrol with a *Visa*-approved Qualified Independent Security Assessor (QISA) who can help guide you through the entire compliance process.
 2. Undertake an online annual PCI Self-Assessment Questionnaire to evaluate and improve the security of your internal systems, business procedures and websites.
 3. Complete a quarterly network scan – using an automated program that checks systems for vulnerabilities – which must be validated by a QISA.

Merchants should begin the validation process by visiting www.visa.ca/ais, where you can: determine your compliance level and requirements; find a list of QISAs; and download the self-assessment questionnaire, guidelines for the network scan and a PDF version of the PCI Data Security Standard.

Safe harbour protection

Once merchants receive written notification from TD Merchant Services that they need to comply with AIS, they have up to one year to complete the required activities. Once AIS-compliant,

a merchant will be granted “safe harbour” from any penalties, fees and fines by *Visa* Canada in the event of a hack or compromise.

The AIS program is part of *Visa*'s “seamless security” effort, which means that, no matter where you are in the transaction process, there are security measures in place to protect *Visa* cards and account information. These layers of protection mean increased customer confidence. Ensuring the security of your *Visa* card data helps you to thwart criminals, build customer trust and ultimately improve your bottom line. ■

Privacy matters: How to keep your business secure

Safeguarding your customer data is important, but so is protecting your private business information. Here are some helpful guidelines to help you maintain confidentiality.

- **Protect onsite ID.** Try to limit the number of staff members who have access to computer passwords, office keys and building entry codes. This information is best given out on a need-to-know basis.
- **Monitor sensitive documents.** When faxing, photocopying or receiving mail, always pick up pages promptly and file away carefully. At the end of the day, remove all sensitive materials from your work area and lock them in the appropriate drawers or file cabinets.
- **Encrypt email.** Electronic mail passes through one or more servers where administrators can easily read it and, if archived, is accessible to hackers for days, months – even years. If sending confidential information via email is unavoidable, consider using encryption software to enhance privacy.
- **Be discreet by phone.** Also try to avoid sharing sensitive information by voicemail, cell phone or speakerphone – it could very easily fall into the wrong hands. In fact, cell phone conversations can be picked up with a good scanner.
- **Use a shredder.** Business papers no longer in use should be shredded before recycling. Confidential information stored on old computers, CDs, DVDs or other storage disks should also be erased before discarding.
- **Screen smarts.** Angle computer monitors – or attach privacy filters or visors – so that only the operator can read on-screen information.

Visit our new website

www.tdcanadatrust.com/merchantservices

Have you had an opportunity to visit our website recently? If you haven't, you're in for a pleasant surprise. We've improved the site's navigation to make it easier for you to find answers to your questions and solutions for your business needs.

In addition, we've enriched the site's content to bring you more of the information you need to make your business grow and prosper. Here are some highlights of what you can expect from the new website:

Easy application

Merchants can now apply for point-of-sale (POS) processing services and related products simply by clicking on "Apply Now," downloading and filling out the application form, and then printing and faxing the completed form to TD Merchant Services.

Valuable resources

The new "Resource Centre" offers a variety of useful resources, including:

- Informative brochures and guides
- Administrative forms (such as change of address/phone/fax)
- Industry information (such as chip technology updates)
- Links to other TD Canada Trust websites, merchant associations and payment industry partners
- Press releases

Helpful tools

In the handy "Tools and Resources" box, you'll find quick links to:

- At-a-glance POS terminal comparison chart

- Fraud prevention brochure
- Back issues of the *Contact* newsletter
- Online reporting, and more

Next time you visit our website (www.tdcanadatrust.com/merchantservices) be sure to add it to your bookmarks or favourites list. ■



Chip card update

As we reported in our last issue, members of Canada's payment card industry – **Visa Canada Association, MasterCard Canada Inc. and Interac Association** – are working together to introduce chip technology to the Canadian market over the next several years. This new technology promises to bring added security and convenience to merchants and consumers alike.

In November 2006, these Canadian payment associations announced plans for a chip technology market trial to start in the fall of 2007 in Kitchener-Waterloo, Ontario. At that time, chip-enabled credit and debit cards will be introduced to Kitchener-Waterloo consumers, while many local merchants will receive chip-enabled POS terminals, training sessions and technical support.

This trial will provide an ideal opportunity to:

- Fine-tune chip procedures and processes before a large number of cards are issued into the national market.
- Test the chip infrastructure and ensure the inter-operability of cards and terminals.
- Develop helpful best-practice guidelines for the rest of Canada.

Throughout the trial, and for some time to come, chip cards will continue to have a magnetic stripe, allowing merchants with magnetic-stripe-only payment terminals to accept payments as usual.

Closer to the trial date, TD Merchant Services will contact merchants in the Kitchener-Waterloo area with all the necessary information. Also watch for updates on our conversion to chip technology in future issues of this newsletter or by visiting www.tdcanadatrust.com/merchantservices

How to protect your PIN pads

Interac Association has one of the most secure networks in the world. In fact, 99.9% of all transactions are conducted without issue, according to the latest figures available from Interac Association.

The “Protect Your PIN Pads” campaign is the Association’s most recent initiative to keep the services secure and help protect merchants and cardholders from fraud. Here’s how you can protect your PIN pads:

- Inspect your POS equipment regularly. If anything looks unfamiliar, appears altered, or is missing, notify TD Merchant Services immediately.
- Ensure you provide customers with enough room to comfortably shield the PIN pad when entering their number.
- Make sure that any security cameras on your premises don’t capture the PIN that customers are entering.
- Allow the customer to hold the PIN pad until the transaction is complete, and never enter a PIN for a customer.
- Check ceilings, walls or shelves near PIN pads on your premises for holes that could conceal a small camera.
- When not in use, place the PIN pad under the counter or out of customers’ reach (but do not unplug).

For more PIN pad protection tips, please visit www.interac.org ■



Whatever your business, protect your PIN pads

Reputation is everything. So understandably, you want your customers’ shopping experience to be a pleasant one. To ensure they don’t become victims of debit card fraud, here are a few simple measures you can take:

- Protect your PIN pads. They’re as good as cash to criminals.
- Check your PIN pads regularly for anything unusual.
- Remind your customers to protect their PIN when entering it.
- Talk to TD Merchant Services about other steps you can take to guard against debit card fraud, or visit interac.org for more tips.



Preferred paper suppliers

The following companies are preferred suppliers of paper for TD Merchant Services point-of-sale terminals. To ensure that you’re dealing with a reputable dealer, give one of them a call when you need paper.

- Main-Tech Industries, 1-800-268-5120
- Maxwell Media Products, 1-800-561-6406

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.

♻️ Printed on recycled paper.

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

* Visa International Service Association/Used under license.
™ Trade-mark of Interac Inc., TD Canada Trust authorized user of Trade-mark.

© Registered Trade-mark of Interac Inc., TD Canada Trust authorized user of the Trade-mark.
© 2007 The Toronto-Dominion Bank, All Rights Reserved.

TD Merchant Services