Stopping fraud before it starts.

Protect your PIN pad, protect your customers.

Interac®

Guarding your business from debit card fraud.

Debit card fraud techniques

Interac debit card fraud losses as a result of skimming are at a record low, decreasing to $29.5 million in 2013 from a high of $142 million in 2009. Only 25% of losses in 2013, or $7.3 million, are the result of fraud exploitation in Canada. Thanks to sound policies, investments in technology, and collaboration with financial institutions, Acquirers/Payment Service Providers, merchants and law enforcement, the *Interac* system is a world class payment network.

Though the statistics clearly show the success of the *Interac* system in reducing *Interac* debit card fraud, it is important for merchants to be aware of the methods criminals are using to commit payment card fraud so you can avoid this from occurring at your business.

Magnetic stripe skimming
Hidden equipment such as card reading devices and pinhole cameras are installed at ABMs or retail locations to collect the magnetic stripe data and PIN of an unsuspecting cardholder. The information is then copied onto a counterfeit magnetic stripe debit card and used with the captured PIN to withdraw money out of the cardholder's account through non-chip ABMs and point-of-sale devices.

Tampered PIN pads
Criminals steal store PIN pads, tamper with the internal components and then place them back into the store enabling criminals to capture the magnetic stripe and PIN information when it is being entered by the cardholder. To do this, the criminals switch the legitimate PIN pad with a fake identical version so that the merchant does not notice it is missing. The criminals return to the store and place the tampered device back into its original location, where they are then able to wirelessly download the card information.

Be mindful

- Criminals will distract employees by buying bulky items or by preoccupying staff while an accomplice accesses the PIN pad.
- They will also look for unattended devices left on the counter.

Everyone has a role to play in preventing fraud
Fraud affects everyone, including merchants. If your customer's debit card is compromised, or if your PIN pad is stolen at your location, your brand or business may suffer. The brand equity that your company has carefully built over time can quickly be eroded as consumer and media reaction is typically swift and negative.

While Interac Association, the financial institutions and law enforcement work together to maintain the security of the *Interac* services, merchants can also play a significant role in the fight against fraud by performing some simple routine inspections around the terminal and cash register area.

What you can do to prevent debit card fraud from happening at your location.

Treat your PIN pad like cash

The PIN pad is just as valuable to criminals as cash.

- Keep PIN pads out of sight when not in use.
- If you have a separate terminal that is not integrated with your cash, lock it up at the end of the day.

Carry out daily checks

Criminals use a variety of techniques to install illegal devices into your store. Conducting routine site inspections is an important practice that will allow you to uncover suspicious devices right away and potentially prevent fraud.

- Check the serial number to ensure your PIN pad has not been stolen and replaced with a decoy.
- Check the surrounding cash area for signs of hidden pinhole cameras (e.g., in ceiling tiles, walls or signs), and unexplained wires.
- Check for signs of tampering (e.g., broken parts, security seals, extra stickers, PIN pads that look like they have been replaced with a brand new back).
- If you have a Fraud Inspection Tool (FIT) card, insert the card in the chip reader and make sure it doesn't pass the black line.

What you should do

If a criminal approaches you and asks you to turn a blind eye or to assist with the installation of a tampered device;

- Politely refuse and advise them that you won't take part in their illegal activity.
- Obtain as much information on the individual(s) such as a physical description, vehicle they drove and license plate.
- Contact law enforcement and your Acquirer/Payment Service Provider immediately.
- Do not place yourself in any danger.

Know your employees/coworkers

Implementing strict hiring procedures is an important step in fraud prevention. In some instances, a criminal may find their way into your organization if proper due diligence procedures are not in place. In other instances, an employee may be approached by a criminal who has them install fraudulent equipment or carry out illegal activity by paying them or threatening them. Steps you can take:

- Ask for government issued photo identification.
- Take a picture of each new employee when hired and maintain a copy of all employee photos.
- Request that all new hires undergo a background check.

What to do if you discover something suspicious or your PIN pad/POS terminal has been stolen

- Do not disturb the potential crime scene.
- Do not touch the device.
- Contact local law enforcement and your Acquirer/Payment Service Provider immediately.
- Cooperate with investigators/law enforcement by providing access for site inspections, shift schedules, employee information and surveillance video footage.

Interac Association can assist you

- A training video is located at interac.ca/fraudvideo.
- Security Seals — Contact your Acquirer/Payment Service Provider to place an order for FREE security seals.
- The Point-of-Purchase Integrity Checklist is located at interac.ca/FraudIntegrityChecklist.

For more information, please contact us at dcfprevention@interac.ca.

INT 005-1174 / E