InteracChip.ca

Transitioning to Chip Technology

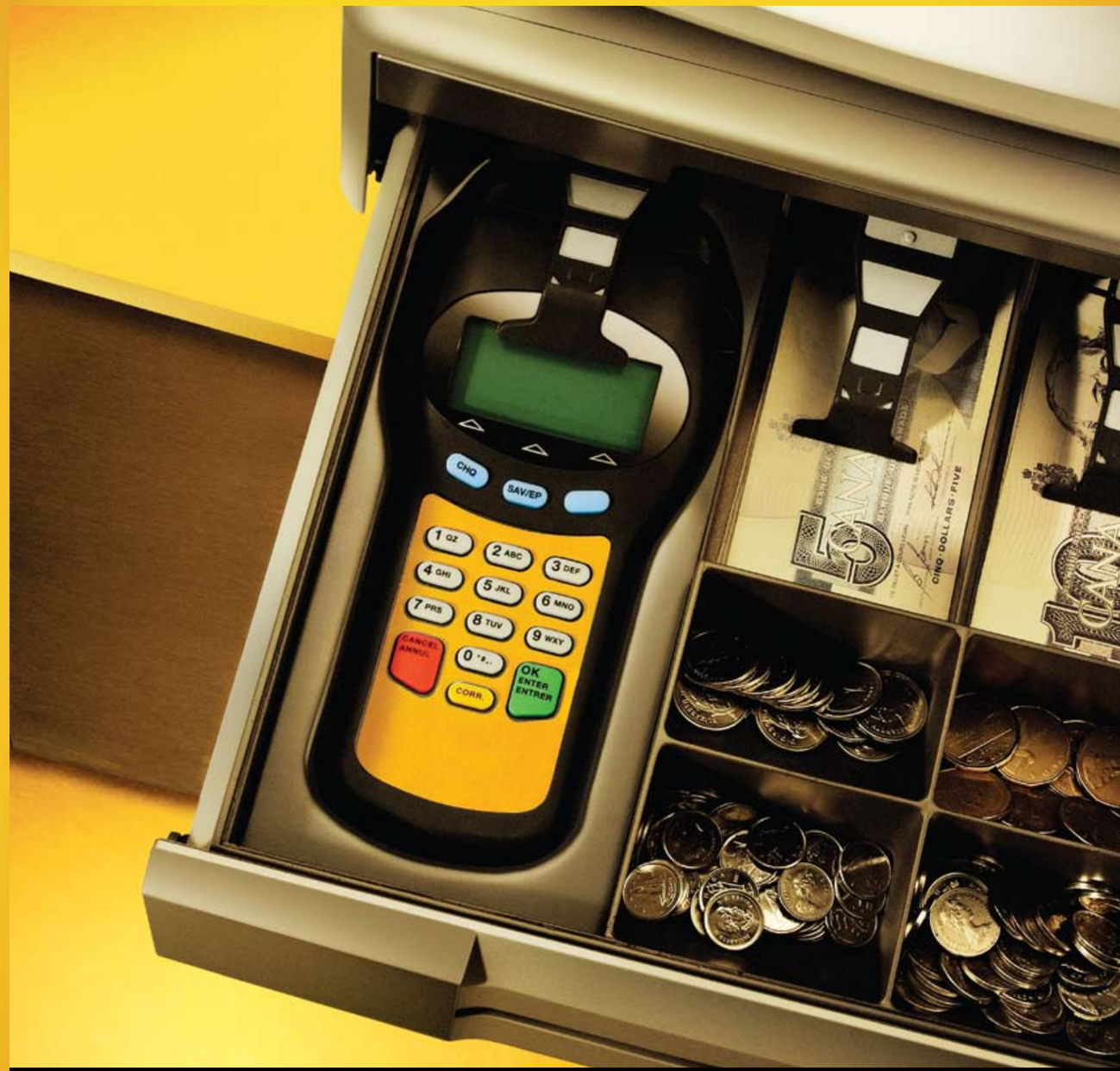
Over the next several years, debit cards, ABMs and point-of-sale devices will be evolving to a new generation of payment card technology, know as chip technology, which will make a safe payment system even more secure. Debit cards will begin to contain an embedded microchip, which will put the power of a computer onto the card. The microchip will give the card the ability to store and process data and communicate with the ABM or point-of-sale device, providing an additional layer of security for your customers. For more information, please visit www.interacchip.ca.

Everyday Simply™

About Interac Association

Interac Association is responsible for the development and operation of Canada's national debit network that provides Canadians access to their money through Automated Banking Machines and stores across Canada. For more information, please visit www.interac.ca.

Protect Your PIN Pad, Protect Your Customers



Debit Card Fraud Prevention

Protect your PIN

Each day, millions of Canadians choose *Interac* Direct Payment for their everyday purchases. In fact, Canadians are among the highest users of debit cards compared to other countries around the world, with one out of every two Canadians selecting *Interac* Direct Payment as their preferred method of payment.

While the *Interac* network is one of the safest systems in the world, debit card fraud, or what is also known as debit card skimming, can occur.

What is debit card fraud?

Debit card fraud is the unauthorized copying of electronic data from a debit card which is then copied onto a counterfeit card and used to withdraw funds without the knowledge of the cardholder. Fraudsters need two pieces of information to produce a counterfeit card – the magnetic stripe information and the PIN number.

Debit Card Fraud Techniques

1 Skimming

Hidden equipment, such as card reading devices and pin-hole 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 card and used with the captured PIN to withdraw money out of the cardholder's account.

What to look for:

- Look for tiny holes in ceiling tiles, adjacent walls, plaques, signs.
- Unexplained wires and an extra card reader.

2 Tampered PIN Pads

Fraudsters steal store PIN pads, tamper with the internal components, then place them back into the store, enabling fraudsters to capture the magnetic stripe and PIN information as it is being entered by the cardholder. To do this, the fraudsters switch the legitimate PIN pad with a fake identical version, so that the merchant does not notice it is missing. The fraudsters 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.

What to look for:

- Fraudsters will distract employees by buying bulky items or by preoccupying staff while an accomplice accesses the PIN pad.
- Broken parts or broken security seal on the device.

Pin-hole camera in a ceiling tile used to film the PIN as the customer enters it into the PIN pad.

Card skimming devices used to copy the magnetic stripe information are tiny and can even be carried by employees.

Fraudster using Bristol board and toilet rolls to block the view of the other fraudster switching the PIN pads.

Tampered security seal

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*, 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:

1 Treat your PIN pad like cash

The PIN pad is just as valuable to fraudsters 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.

2 Carry out daily checks

Fraudsters 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.
- Check the surrounding cash area for signs of hidden pin-hole cameras, e.g. 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.

3 Know your employees/coworkers

Implementing strict hiring procedures is an important step in fraud prevention. In some instances, a fraudster 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 the fraudster who has them install fraudulent equipment or carry out illegal activity by paying them or threatening them.

- 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 merchant service provider immediately.
- Cooperate with investigators/law enforcement by providing access for site inspections, shift schedules, employee information and surveillance video footage.

For more information about debit card fraud prevention,
please contact Interac Association at dcfprevention@interac.ca or your payment service provider.