Putting The Brakes On Fraud

Protect your PIN pad, protect your customers

GUARDING YOUR BUSINESS FROM DEBIT CARD FRAUD

Debit Card Fraud Techniques

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.

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.

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.

Be Mindful Of

- Fraudsters 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 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

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. 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)

What You Should Do

If a fraudster approaches you and asks 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 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 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 Can Assist You

- Training Video located at www.interac.ca/fraudvideo or USB stick
- Security Seals - Contact your merchant provider to place an order for free security seals
- Integrity Checklist

For more information about debit card fraud prevention, contact your Acquirer/Payment Service Provider or dcfprevention@interac.ca.

Interac®

Everyday Simply®

N 003-12-1007 / E