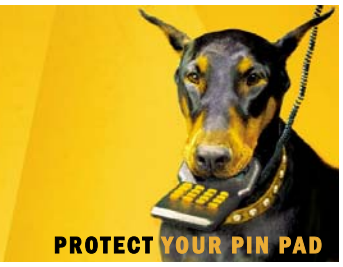
Merchant Best Practices to Deter Skimming at Retail Locations



What is Debit Card Skimming?

Debit card skimming is the transfer of electronic data from a customer's debit card to another source for fraudulent purposes.

Purpose

The purpose of this document is to identify and describe Best Practice activities for **retail managers/employees** to combat debit card skimming.

Best Practices - Why bother?

Debit card skimming affects everyone, from merchants to customers. It is in everyone's best interest to prevent debit card skimming to avoid putting your reputation and your customers at risk. The Best Practices outlined here will help you to prevent debit card skimming at your location.

Best Practice Activities

Hiring

- Always obtain all information for each staff member, including full name, date of birth, current resident address/telephone number and Social Insurance Number (SIN).
- Every new hire must complete a detailed application including previous employment, home address and references. Hiring managers should ensure that the information provided by new hires is true and accurate.
- Government issued photo identification must be presented to the manager for each new hire. Keep a photocopy of the identification or take a picture of each new employee at the time of hiring them and maintain a copy of all new hires.
- Conduct thorough in-person interviews with each new applicant. Your organization may utilize new employee testing or screening to help identify the best candidates.
- Inform each new hire that skimming is a criminal offence and will not be tolerated.

Red Flags – Be cautious if:

- the only phone number a new hire provides is a cell phone.
- new hires cannot present photo ID.
- new hires only want to work midnight shifts.

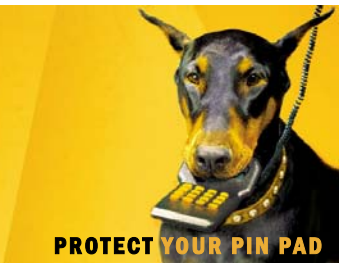
Employee Monitoring

- Maintain accurate shift schedules, including last minute changes, for at least 12 months.
- Make employees accountable by requiring them to write their name or employee number of the back of each legitimate transaction draft.
- Make random visits during evening or weekend hours when managers are not usually present, as these are the times most debit card skimming occurs.
- Review surveillance films on a regular basis, especially when new hires begin work on off-peak hour shifts.

Red Flags – Be cautious if:

- employees seem scared to allow device inspections or afraid to answer questions about suspicious customers.
- employees quit suddenly and leave a pay cheque behind. Alert your supervisor and/or payment service provider immediately!

Merchant Best Practices to Deter Skimming at Retail Locations (Continued)



Equipment and site inspection

- Conduct inspections daily.
- Refer to the Recommended Checklists for step-by-step inspection techniques.

Red Flags – Be cautious if:

- anything on the ceiling appears different, pin-hole cameras for capturing customers' PINs can be installed in ceiling tiles.
- ceiling tiles have been moved or if new wires appear behind the ceiling tiles.
- cash registers or devices for processing debit card transactions have been removed and/or fixed in a stationary location.

Equipment

- Install security seals (also called tamper proof labels) on all sides of any keyboard, keypad or any other device used for processing debit card transactions. If these seals are removed or disturbed, contact your Acquirer and law enforcement immediately.
- Maintain an accurate and up-to-date list of serial numbers for all devices and check devices randomly to ensure numbers are the same.

Protect your PIN material

Display Protect your PIN stickers on POS devices.

Escalation procedures with law enforcement

- Know the procedures within your company for contacting corporate security or territory managers.
- Know who to contact in law enforcement and at your company if tampering is detected.
- Cooperate with investigators/law enforcement in terms of site inspections, providing shift schedules, employee information and surveillance camera tapes.

Communication

- Stay current on trends in debit card fraud by reviewing, Acquirer and Interac Association updates or newsletters.
- Make sure you know the appropriate procedure to report suspicious activity, damaged or compromised devices.

Checklist sign off

A sign off sheet for completion of skimming prevention tasks (device inspections, employee monitoring) to submit to either head office or territory manager, as directed by your supervisor/manager or head office included in this package (see Point of Purchase Integrity Checklist).

Commitment to Best Practices

Using these principles will help protect your business and your customers.

FOR MORE INFORMATION, PLEASE CONTACT YOUR ACQUIRER OR SERVICE PROVIDER