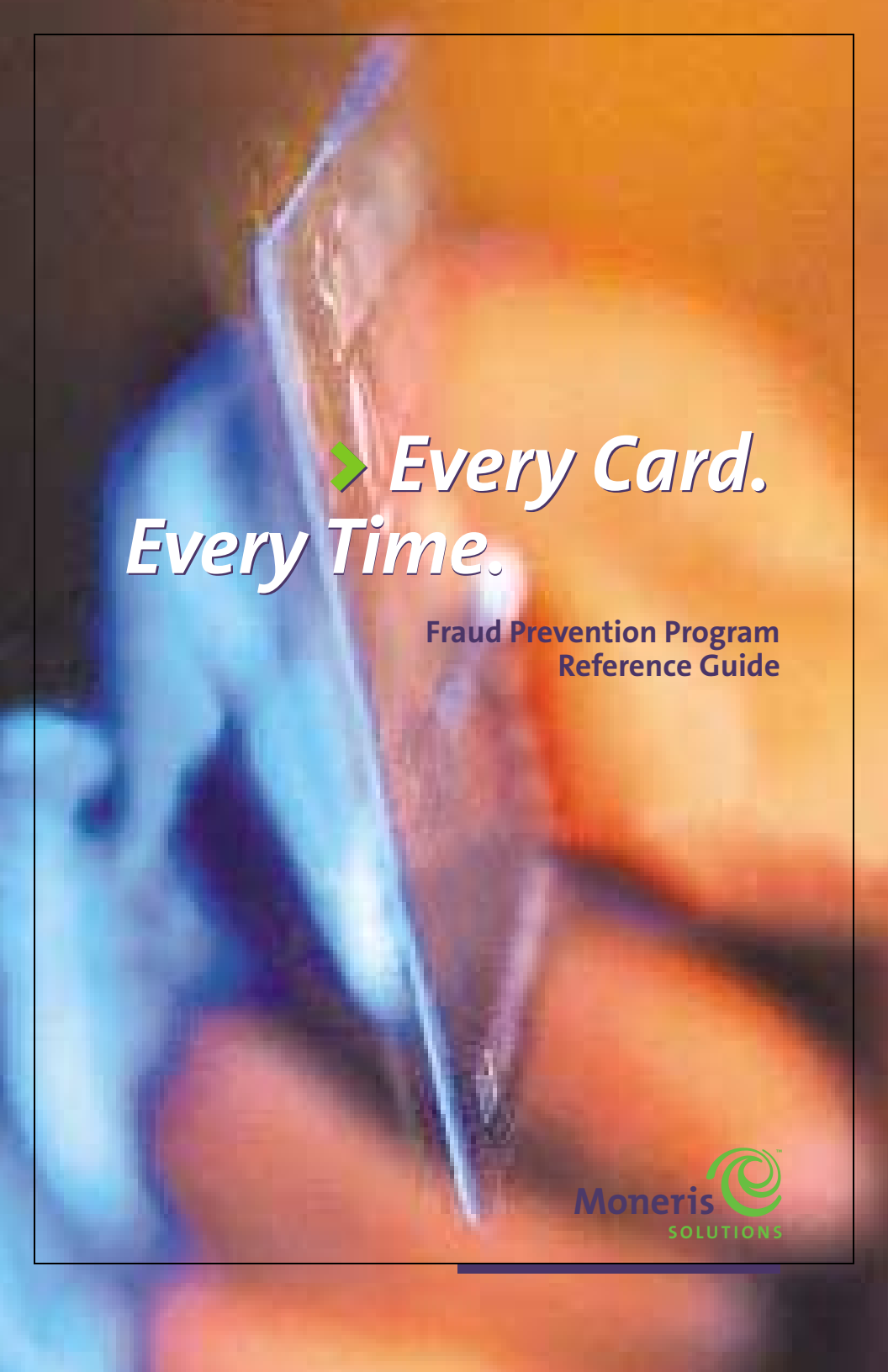

Every Card.
Every Time.
Fraud Prevention Program
Reference Guide
Moneris
SOLUTIONS

> Every Card. Every Time.

Table of Contents

Welcome to the Moneris Solutions Fraud Prevention Program.

In this Reference Guide you will find everything you need to help minimize credit card fraud. Fraud is an ongoing issue that hurts us all, and could have significant financial implications for your company.

The most effective way to reduce fraud is through employee education and training. Store clerks who accept the customers' debit and credit cards need to know what to look for and what actions to take if they are suspicious of fraud. Once employees are aware, they need constant reinforcement of the message and we hope our slogan "Every Card. Every Time." is a useful reminder. Like any good habit, staff behaviour can easily slip back into sloppy card handling if the staff and store are busy.

This Guide covers the following topics in detail:

- *Suspicious customer behaviour*
- *Card security features*
- *Proper processing procedures*
- *Code 10 Procedures*
- *Mail/Telephone Order and Internet fraud*
- *Skimming*

Please post the ongoing promotion materials in a lunch room or other staff area, the reminder card near the POS and place the tent card in a visible spot at checkout.

Once staff has been trained on proper processing procedures, management needs to encourage staff to use common sense, and to follow their instincts. While some fraud activity is quite sophisticated due to today's plastics technology, your front-line staff can make a huge difference with something as simple as calling for a Code 10 authorization.

It's important that the message about fraud prevention tactics comes from an employee's direct supervisor. It needs to be engrained that being vigilant against credit card fraud is a "must do" element of the job.

1

Suspicious Customer Behaviour

Be alert and observe your customers.

Detecting credit card fraud begins with keeping your eyes and ears open. Bad cards can be broadly classified into two groups. The first category is lost or stolen cards, where the card is legitimate, but the user is not the authorized cardholder. The second is counterfeit cards, where the card is illegally produced but looks and works like a legitimate card.

Our experience shows that the perpetrators of credit card fraud often display the following characteristics:

LOST OR STOLEN CARDS

Indiscriminate purchases

- The customer has randomly collected merchandise and may appear nervous or in a hurry.
- The customer may make purchases just as the store is closing.
- The customer does not take the care usually associated with making a purchase.
- In a clothing store, the customer may have chosen merchandise without regard to size, colour, style or price. They may not have tried the items on.
- When purchasing expensive electronics, they may not ask about technical specifications or warranties.
- For large items, they may take immediate delivery and not request assistance.

The card

- The customer may take the card from their pocket instead of a wallet or purse.
- The customer may sign the sales draft in a deliberate or unnatural way.
- The signature on the card and the draft may not match.
- The card may have a female name but be used by a male, and vice versa.
- The customer may randomly charge expensive items on a newly valid card.

"Detecting credit card fraud begins with keeping your eyes and ears open."

COUNTERFEIT CARDS

Confidence

- The customer will look the part of a customer who purchases expensive items. They will likely be well-dressed and self-confident.
- They are confident their purchases will be approved given they are a part of the production of these high-quality cards.
- They may spend a lot of time browsing and very often pick up merchandise the following day.

Come back for more

- The customer will frequently return with friends, who also have counterfeit cards, claiming they find the merchandise and prices attractive.

Important note

- *Any of these characteristics can be present in a legitimate transaction, just as the absence of these characteristics does not guarantee a legitimate transaction. Common sense is always the best guide.*
- *If you or your staff have any doubts or suspicions, give yourself, not the customer, the benefit of the doubt. Call for a Code 10 authorization (See page 17) which is used when you suspect a card transaction may be fraudulent, or should be given a closer look.*

2

Card Security Features

KNOW WHAT TO LOOK FOR

All credit cards are designed with special security elements to deter counterfeiting and alteration. When you are presented with a card, look for the following elements:

ALL CARDS

Verify the match of print and embossing

Do the pre-printed digits match the first four digits of the embossed account number?

Embossing

The embossing should be clear and uniform in size and spacing.

Hologram

Are the four last numbers of the card embossed in the hologram?

Valid Date

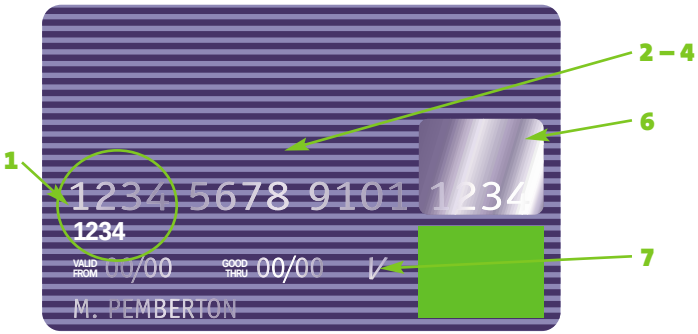
Does today's date fit between the effective and expiry dates? The card is valid until the last day of the month shown.

Compare account numbers

Is the account number embossed on the card exactly the same as the account number printed on the sales draft and displayed on the terminal (if equipment allows)?

SPOTTING A BAD CARD (FRONT)

Today's technology can help fraud artists alter or counterfeit cards. You can outsmart them by looking for these signs:



1. A mismatch between the printed four-digit number and the first four embossed numbers
2. Embossed characters that are enlarged or out of proportion to the other characteristics on the same line
3. Numbers or letters that are ill-defined or of varying type styles
4. Inconsistent spacing or crooked embossed lines
5. A printed surface that is chipped or scratched
6. The absence of a three-dimensional hologram
7. The absence of a stylized V (VISA) and MC (MasterCard) on the card
8. Silver or gold paint used to touch up the hologram after re-embossing the account number

ELEMENT	VISA	MASTERCARD
Account Number	Does it begin with a “4”?	Does it begin with a “5”? Is it 16 digits?
Security	All VISA cards show a stylized “V”. Some cards may have one other letter prior to the V.	All MasterCard cards have a stylized “MC” embossed on the line next to the valid date
Hologram	Does a dove appear to fly when the card is tilted in light?	Do the interlocking globes showing three continents move when the card is tilted? Does the word “MasterCard” appear in the background of the hologram?

SPOTTING A BAD CARD (BACK)

- The word "VOID" exposed by an erasure of the signature panel
- Damage to the word mark pattern on the signature panel, or no pattern at all
- Glued-on paper, white adhesive tape or paint covering the original signature panel

"All credit cards are designed with special security elements to deter counterfeiting and alteration."

ELEMENT	VISA	MASTERCARD
Signature Panel	Is the word "VISA" repeated at an angle across signature panel?	Is the word "MasterCard" repeated at an angle across signature panel?

ALL CARDS (BACK)

Signature Panel

Is the account number (VISA) or the last 4 digits of the account number (MasterCard) printed in reverse italics on the signature panel? Is it followed by a 3-digit card validation code?

Signature

Is signature panel signed? If it is not signed, ask the cardholder to sign the card and compare that signature with one on a valid government-issued I.D.

Does the signature on the back of the card reasonably compare with the signature on the sales draft?

3

Proper Processing Procedures

REMEMBER THE BASICS

By following proper processing procedures, you reduce the chance of fraud:

- Look at the hologram, the four-digit printed bank identification number, the unique embossed symbol and the signature panel.
- Check the card expiration date.
- If you use a terminal to authorize credit card transactions, swipe the card through it. Check the terminal's display of the account number encoded in the card's magnetic stripe and compare it with the account number embossed on the card.
- If you are satisfied that the card is genuine, use your normal authorization procedures to request approval. Do not give the card back to the customer until the authorization procedure is complete.
- Have the customer sign the draft in full view.
- Compare the signature on the card with the signature on the draft for similar handwriting.

ALWAYS SWIPE THROUGH A TERMINAL

- It's faster and helps to prevent fraud.
- Swipe card once and in one direction only. Do not slide it back and forth.
- Compare account numbers. Do last four digits of account number on sales draft match last four digits of embossed account number? If not, phone the Moneris authorization centre at **1 866 802 2637** and follow the prompts for a Code 10 authorization.

- If you receive a message of "Call" or "Call Centre", call the authorization number. If you suspect fraudulent activity, or have any questions regarding transaction approval, ask for a Code 10 authorization.
- If the authorization centre requests that you retain a customer's card, do so only by reasonable and peaceful means. Never put yourself in danger.

When a card's magnetic stripe can't be read, it's usually because:

- the magnetic stripe reader is broken or dirty
- the reader is obstructed, preventing a clean swipe
- the sales associate swiped the card improperly
- the card's magnetic stripe is damaged

MANUAL TRANSACTIONS

- The magnetic stripe is an active component of the card's security that makes manual processing appropriate only when a card's stripe can't be read.
- **When a card's stripe can't be read, a manual sales draft must be completed that includes all of the following:**
  - Date
  - An imprint of the card
  - Details of the transaction
  - Dollar amount
  - Customer signature

Note:

- Do not write "void" or "copy" on the face of the manual salesdraft.
- The card number must then be manually keyed to obtain an authorization.

On the POS terminal receipt you must:

- Print "PROOF COPY" on the signature line
- Record the pre-printed reference number as it appears on the manual sales draft

Retain records:

Copies of both the manual sales draft and the POS transaction receipts are needed to fulfil any retrieval request generated by Merchant Services. Failure to follow these procedures may result in financial loss to your business.

- If a transaction is key-entered, always get a card imprint on the sales draft. In case the charge is later disputed, an imprint proves the card was present, and helps protect you from chargebacks.
- For authorizations, each over-the-floor-limit credit card transaction must be approved, and the subsequent code must appear on the sales draft.
- If the ratio of key-entered transactions to total transactions is greater than one percent for sales associates or card readers, try to determine the reason.
  It's a good idea to monitor your rate regularly.

KEY ENTRY

Key-entered (as opposed to card-swiped) transactions have some real disadvantages:

- The most significant is the increased risk of fraud or counterfeit.
- It can also lead to increased costs, as your merchant discount rate is calculated based on your ability to read and transmit the magnetic stripe data at POS.
- It is less efficient, as transactions take longer to complete and are prone to errors.
- It may lead to lost sales because the authorization decline rates are higher for key-entered transactions, so the potential for lost sales is also higher.

STEPS TO AVOID KEY-ENTRY

- Regularly check the magnetic stripe reader at POS to be sure it is working properly.
- Clean readers periodically with the ReaderClean card that came with your terminal. They can also be purchased at most office supply stores.
- Position readers to facilitate a full card swipe, with any obstructions removed.
- Do not allow staff to place items near readers that could soil or damage these devices, particularly food and beverages.
- Do not place readers near any equipment that deactivates magnetic anti-theft devices attached to merchandise.

TEACH SALES ASSOCIATES THE PROPER WAY TO SWIPE A CARD:

- Before swiping, make sure the stripe is facing the reader.
- Always swipe the card once in the direct of the arrow shown on the reader.
- Never swipe a card back and forth or at an angle, as it may cause the reader to misread the stripe.

HELP CUSTOMERS "PROTECT YOUR PIN"

Interac has developed a campaign to raise cardholder awareness and trigger their behaviour around PIN protection at point of use.

WHAT YOU CAN DO TO REDUCE PIN THEFT

Ensure the terminal is installed so that your customers can easily shield the PINpad while entering their Personal Identification Number.

Allow your customers to hold the PINpad until they receive the final approval/decline response message.

Always give your customers a copy of the transaction record and return their banking (debit) cards to them.

If the terminal is not working, please check the following before contacting Moneris:

Are the electrical and telephone connections in place?

Does the terminal have recording paper?

Are the telephone lines working?

CONSIDER ADDING A COUNTERFEIT AND FRAUD DETECTION DEVICE TO YOUR FRAUD PREVENTION MIX

Additional security products may also help prevent credit card fraud. All major credit cards contain security features that are invisible to the eye under normal lighting conditions, but easy to spot when held under the special light of fraud detection equipment. SecuriSource, a manufacturer of security products, offers the ID-2000 Counterfeit Detector designed to cut losses. The device works for US and Canadian currency, all major credit cards, and all cheques and gift certificates encoded with special security features. Its visible presence will act as a deterrent against counterfeit and fraud, and is most effective when kept at every point of purchase where credit and cash transactions are made.

Check out their website ***www.securisource.com****, or call* ***1-800-866-5166*** *for details. Moneris Solutions has negotiated a preferred pricing arrangement for Moneris Merchants with SecuriSource.*

4

Code 10 Procedures

Code 10 is a universal code that allows merchants to alert an authorization centre of a suspected fraudulent transaction without alarming the individual who is presenting the card.

PROTECTING YOUR BUSINESS

Even when proper procedures are followed and a card is swiped, and a matching signature is obtained on the sales draft, there is no guarantee that it is a legitimate transaction. If there is any suspicion of fraud, initiate a Code 10 authorization.

In most cases, transactions are legitimate, but you should know what to do in the event of a Code 10:

- Call the Moneris authorization centre at **1 866 802 2637** and follow the prompts for a Code 10.
- Identify the call as a Code 10.
- Hold the card in your hand during the authorization process. Stay calm and remain casual and courteous with the customer.
- Your call may be transferred. Please do not hang up.
- you will be asked a series of yes or no questions to verify the authenticity of the card.
- Follow the instructions given to you over the telephone.
- Do not try and apprehend or detain the cardholder.
- A reward may be paid for the return of a lost, stolen or counterfeit card.

If for any reason you become suspicious of a transaction or cardholder, call the Moneris authorization department. Code 10 procedures have been developed for your protection.

Trust your instincts and always err on the side of caution.

5

Mail/Telephone Order and Internet Fraud

Many of the safeguards against fraud in traditional retail environments do not work in situations where the card is not present, including mail/telephone orders (MOTO), and the world of e-commerce. These transactions do not require face-to-face contact or an actual card in hand, so there is more anonymity.

All MOTO and Internet merchants must authorize their transactions. If funds are available and a card has not been reported lost or stolen, the transaction will most likely be approved by the issuing bank. For merchants, it is important to remember that an authorization is not proof that the true cardholder is making a purchase or that a legitimate card is involved. An authorization only means that credit is available and that the card is not currently blocked. To detect fraud, authorizations must be augmented with the right combination of tools and controls.

IF YOU SUSPECT FRAUD

If you are suspicious of a transaction, ask the customer for additional information:

- day and evening telephone numbers, which can be verified through Directory Assistance or www.canada411.ca
- additional information such as the bank name on front of card
- separately, confirm the order by sending a note via the customer's billing address, rather than the "ship to" address.

MOTO FRAUD

Merchants are open for chargebacks with this type of processing. Any disputes will be returned, regardless of what was verified or investigated. The only exception is the *Verified by VISA* program.

VERIFIED BY VISA

Merchants must register and be approved for *Verified by VISA*. The objective of this program is to guarantee the transaction as a legitimate one for the merchant by transferring liability to the issuing bank, and therefore minimizing chargebacks.

This password verification process allows the cardholders' identities to be confirmed in real-time during checkout by the cardholder's financial institution. It is meant to closely replicate a "card present" environment, which can help to reduce the risk of fraud.

Verified by VISA is initiated when the cardholder proceeds to your checkout page and clicks "buy". The program creates a window for the cardholder to enter their password. The cardholder's financial institution can then authenticate the cardholder and send you the response needed to proceed with payment authorization.

"Many of the safeguards against fraud in traditional retail environments do not work in the world of e-commerce."

INTERNET FRAUD – WHAT TO WATCH OUT FOR:

- Internet merchants should never accept orders via email, even if your site is secure, because the card data is exposed from the cardholder's end.
- First time shoppers – criminals are always looking for new victims.
- Larger-than-normal purchases – because stolen cards or account numbers have a limited life span, thieves need to maximize the size of their purchases.
- Orders consisting of several of the same item – having multiples of the same item increases the criminal's profits.
- Orders placed using numerous credit cards – transaction is split between several cards.
- Orders placed on cards issued by a country different than the country the goods are shipped to (e.g. orders on Australian cards and goods shipped to Bulgaria).
- Orders made up of "big-ticket" items – these items have maximum resale value and therefore maximum profit potential.
- Orders shipped "rush" or "overnight" – thieves who want to quickly resell items aren't concerned about extra delivery charges.
- Orders from Internet address making use of free e-mail services. For these services, there's no billing relationship and often no audit trail or verification that the legitimate cardholder has opened the account.
- Orders shipped to an international address – a significant number of fraudulent transactions are shipped to fraudulent cardholders outside North America.

HOW TO STAY "CYBERSAFE"

- Develop and maintain a customer database or account history files to track buying patterns and compare individual sales for signs of possible fraud.
- Establish and enforce appropriate controls on the employees who have access to the customer database and account numbers.

WATCH FOR:

- Transactions on account numbers that seem to follow a pattern.
- Orders shipped to a single address but made on multiple cards – these could also be characteristic of an account number generated using special software available on the Internet, or a batch of stolen card numbers.
- Multiple transactions on one card over a very short period of time – this could be an attempt to "run" a card until the account is closed.
- Multiple transactions on one card or similar cards with a single billing address, but multiple shipping addresses – this could represent organized activity, rather than one individual at work.
- Multiple cards used from a single IP (Internet Protocol) address – more than one or two cards could well indicate a fraud scheme.

WHAT TO DO IF YOUR CREDIT CARD DATA IS COMPROMISED

E-commerce merchants need to be vigilant at all times against fraud. Hackers and thieves are always looking for holes in security systems, and opportunities to steal valuable information. We know you're doing everything you can to stay "cybersafe", but if you think you have been compromised:

Act fast

- Contain damage and limit your exposure
- Preserve your logs and electronic evidence
- Do not access the compromised system

Investigate

- Within 24 hours, record all actions taken to identify the security breach and possible loss of account information
- Be on high alert and monitor all systems that hold account information.

Contact Moneris

Call Moneris at 1-866-319-7450 and we will work with you to:

- distribute compromised account numbers
- identify the security vulnerabilities
- take corrective action to minimize future risk

It's important that you contact us, because our expert staff will know how to identify the issue and help resolve it. We can also help to minimize the impact that an incident might have on your customers, business reputation and bottom line. We all have a vested interest in protecting the goodwill of our mutual customers.

6
Skimming

Skimming is the transfer of electronic data from one magnetic stripe to another for fraudulent purposes, using card readers. Service stations and restaurants are often the target of skimming, with staff working alone for long periods of time, often at night or on the weekends.

GETTING THE MAGNETIC STRIPE INFORMATION

- There is increasingly sophisticated technology available today that employees use to skim magnetic stripe information from credit and debit cards through either a tampered or dummy terminal.

BE ALERT

- There are now very portable skimming devices that capture card track data running through the host line for authorizations.
- These devices have the capacity to run for days at a time with their larger storage capacity.
- Check under the counter, a convenient hiding spot for skimming devices and activity.

"Service stations and restaurants are often the target of skimming, with staff working alone for long periods of time, often at night or on the weekends."

FOR DEBIT CARDS

In addition to the magnetic stripe information, skimmers also need to obtain the cardholder's PIN number.

This is typically done in the following ways:

- "PIN surfing"– either the employee or an accomplice will "surf" at the moment the customer is keying in their PIN
- A more sophisticated way is the use of a mini-camera lens, placed either in a hole in the ceiling or on a shelf above the counter and the PINpad. With this equipment, the PINpad has to remain in a fixed position on the counter in order for the lens to capture the numbers being keyed in.

PREVENTION

- Most often, a skimming employee works alone on the weekends or at night. Random visits to the store by a manager or lessee will help to reduce fraudulent activity.
- In the case of mini cameras, managers and lessees should check for suspicious holes in the ceiling and/or walls.

EMPLOYEE HIRING AND ACCOUNTABILITY

To prevent employees from getting the chance to skim, it's important to do due diligence with hiring and supervising employees.

New hires

- Full identity of potential employees, including name, date of birth and Social Insurance Number (SIN) should be provided. Ask to see government-issued photo identification.
- There have been numerous cases where a service station job seeker's primary purpose is to skim for a criminal group.

Ensuring accountability

- Meticulously updated schedules should be kept for a minimum of 12 months to enable investigators to determine employees who were on duty at the time of the skimming operation, when legitimate transactions took place. Note that skimming has been reported more than 6 months after the customer used their cards at a suspect POS.
- A significant deterrent to skimming activity is to mandate employees to sign or write their employee number on each legitimate transaction draft.
- Offering a reward to employees who report suspected skimming activity or who are approached by skimming groups is also another effective deterrent.