Every Card. Every Time.

Fraud Prevention Program
Reference Guide

Moneris SOLUTIONS

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
- Best Practices
- Authorizations and refunds
- Code 10 Procedures
- Mail/Telephone Order and Internet fraud
- Skimming

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.

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 employees 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.*

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.

Chip
- Ensure the microchip is embedded on the front of the card

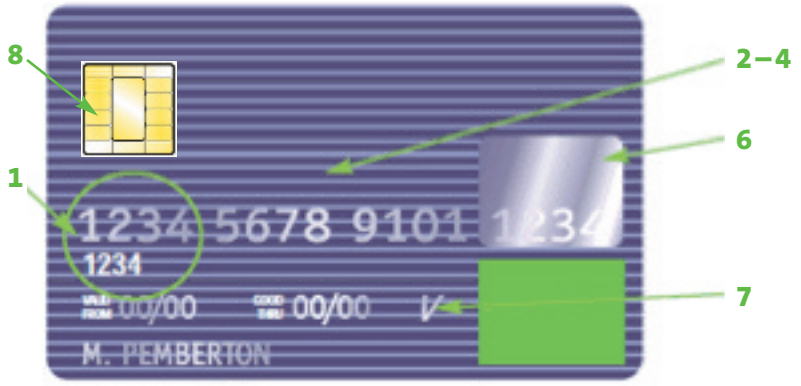
Hologram
- Are the four last numbers of the card embossed in the hologram?

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:



Spotting a bad card (front)

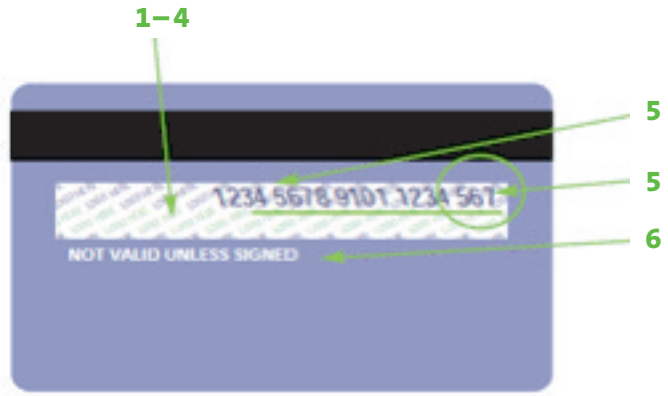
1. A mismatch between the printed four-digit number and the first four embossed numbers
2. Embossed characters that are enlarged or out of proportion to the other characteristics on the same line
3. Numbers or letters that are ill-defined or of varying type styles
4. Inconsistent spacing or crooked embossed lines
5. A printed surface that is chipped or scratched
6. The absence of a stylized V (Visa), MC (MasterCard) or D (DISCOVER) on the card
7. Silver or gold paint used to touch up the hologram after re-embossing the account number
8. The Chip is not embedded or it is glued on the front of the credit card

Spotting a bad card (front)

Element	Visa	MasterCard	Discover
Account Number	Does it begin with a "4"?	Does it begin with a "5"? Is it 16 digits?	Does it begin with a "6"?
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.	All Discover cards have a stylized "D" embossed on the same line as the embossed "member since" date or "year joined" date (if present) and the "valid through" date.
Hologram	Does a dove appear to fly when the card is tilted in the light?	Do the interlocking globes showing three continents move when the card is tilted? Does the word "MasterCard" appear in the background.	A three dimensional hologram on the front of the card or a three dimensional holographic magnet stripe on the back of the card. Valid cards do not display holograms on both front and back

Spotting a bad card (back)

1. The word "VOID" exposed by an erasure of the signature panel
2. Damage to the word mark pattern on the signature panel, or no pattern at all
3. Glued-on paper, white adhesive tape or paint covering the original signature panel
4. The absence of a three dimensional hologram
5. **Signature Panel** – Is the account number (Visa) or the last 4 digits of the account number (MasterCard and Discover) printed in reverse italics on the signature panel? Is it followed by a 3-digit card validation code?
6. **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?



Element	Visa	MasterCard	Discover
Signature Panel	Is the word "Visa" repeated at an angle across?	Is the word "MasterCard" repeated at an angle across signature panel?	Is the word "Discover" or "Discover Network" repeated at an angle across signature panel?

Proper Processing Procedures

Remember the basics

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

- Ensure that the card being presented is valid and that the standard identification and security features of the card have been verified
- Look at the hologram, the four digits printed bank identification number, the unique embossed symbol and the signature panel
- Check the card expiration date
- Check the terminal's display of the account number encoded in the card's Chip and 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
- Proper Card Acceptance procedures must be followed at all times to avoid or mitigate the risk of potential fraud-related chargebacks
  - IF – Terminal is Chip & PIN ready and the cardholder has a Chip & PIN preferring card, merchants must insert the card and obtain a 'Verified by PIN' transaction that is fully authorized (no decline or refer response).

  - IF – Chip & PIN technology fails, merchants must swipe the card. The merchant must obtain a valid authorization and the cardholder's signature, or he or she will be liable for fraud-related chargebacks if the transaction is disputed.
  - IF – Chip & PIN technology fails AND card swipe fails, key in the card number and obtain a valid authorization. A manual imprint of the credit card and the cardholder's signature are required, or the merchant will be liable for fraud-related chargebacks if the transaction is disputed.

  - IF – Terminal is Chip & PIN ready and the card is a Chip & Signature card, merchants must insert the card and obtain a valid authorization and the cardholder's signature on the transaction receipt.
  - IF – Terminal is Chip & PIN ready and the card is a non–chip card (magnetic-stripe only), merchants must swipe the card and obtain a valid authorization and the cardholder's signature on the transaction receipt.
  - IF – Terminal is Chip & PIN ready and the cardholder has a Chip & PIN preferring card but forgets the PIN or PIN is locked and the PIN attempt fails, merchants must advise the cardholder to contact their Card Issuer, or ask for another form or payment.
  - IF – Chip card is removed from the device before the transaction is finished, merchants must re-insert the card and obtain a "Verified by PIN" transaction that is fully authorized.
  - IF – Terminal is NOT Chip & PIN ready and the card is Chip & PIN preferring, merchants will be liable for fraud-related chargebacks, even if proper card acceptance procedures were followed.
  - IF – Merchant is experiencing system failure, downtime procedure for credit cards MUST be followed. Debit cards cannot be accepted during downtime.

Chip & PIN Transactions

- The card is inserted into a chip-reading terminal, instead of being swiped.
- The card remains inserted in the terminal throughout the transaction
- The terminal will display the purchase amount and request the cardholder's PIN
- The cardholder will enter his or her PIN on a keypad
- If the PIN is confirmed, and the purchase approved, a receipt is printed

Magnetic-stripe cards

- For all Non-Chip, card present transactions, the card must be swiped
- Swipe the card once and in one direction only.
- Enter the correct amount to be authorized and verify the authorization response.
- Obtain the cardholder's signature
- 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 the embossed name and numbers do not match those printed on the receipt, request a Code 10 authorization

Note: *For merchants who are not Chip & PIN ready, swiping a chip card does not provide protection from fraud-related chargebacks under liability shift rules*

Signatures

Not obtaining a signature when required could result in a chargeback if the cardholder later denies authorizing the transaction.

- Have the customer sign the draft in full view
- If the signature panel is blank, review valid identification such as a driver's license. Ensure the customer signs the card promptly and decline the transaction if the cardholder refuses.
- Compare the signature on the card with the signature on the draft for similar handwriting.
- If the signatures do not match, request additional identification. If they still don't match, request a Code 10 authorization if you are suspicious of the customer (Please see *Code 10 process* on page 19)
- If the signature varies greatly, ask for additional identification or make a Code 10 call (refer to *Code 10 process* on page 19).

Key-Entered Transactions

The Chip and magnetic stripe are active components of the card's security that makes manual processing appropriate only when a card's Chip or magnetic stripe can't be read. Key-entered transactions are considered high-risk and may result in Chargebacks.

- At the POS terminal you must:
  - Manually key enter the card number.
  - Enter the correct amount and valid expiry date
  - Verify the authorization response
- 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
- A manual sales draft must also be completed that includes all of the following:
  - Date
  - An imprint of the card
  - Details of the transaction
  - Dollar amount
  - Customer signature
  - Authorization Number/Code
  - Merchant name, address and merchant number
  - Do not write "void" or "copy" on the face of the manual sales draft.

Note: *For merchants who are not Chip & PIN ready, an imprint of a chip card does not provide protection from fraud-related chargebacks under liability shift rules.*

Retain records:

- Copies of both the manual sales draft and the POS transaction receipts are needed to fulfill any retrieval request generated by Moneris Solutions
- Failure to follow these procedures may result in financial loss to your business.
- If a transaction is key-entered, always obtain a card imprint and signature on the sales draft.
- Each authorization request 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 1% for sales associates or card readers, try to determine the reason. It's a good idea to monitor your rate regularly.

Manually keyed transactions

Key-entered (as opposed to Chip or 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 Chip or magnetic stripe data at your 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 Chip or 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 Chip insert or full card swipe, without any obstructions.
- 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.

Terminal not working

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?

When the POS electronic system is unavailable, merchants will need to revert to manual processing procedures.

Ensure that procedures for Down Time processing are followed:

Down time procedures:

- If amount is greater than your assigned floor limit, Call Moneris for a voice authorization at **1-866-802-2637**
- Take a manual imprint of the credit card and obtain the cardholder's signature on the manual sales draft.
- Record the authorization number and correct amount on the manual sales draft.
- When system/service is restored, force post the transaction on the electronic POS terminal using the assigned authorization number
- Ensure that all of the information is clearly visible on the manual sales draft

Note: *Do not submit copies of manual sales drafts to Moneris Solutions for processing*

Teach sales associates the proper way

If the cardholder is present and has the card number but not the card, decline the transaction. Even with an authorization, the transaction may be fraudulent and charged back to you.

To insert a chip card:

- Before inserting a Chip card, ensure the Chip is visible.
- Always insert the card in the direction of the arrow shown on the reader.
- Never remove the Chip card prior to completion of the sale.

To swipe a card:

- Before swiping, make sure the stripe is facing 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 and Credit Card issuers have 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 cards to them.

Pre-Authorizations and Refunds

Hotel and Car Rental Pre-Authorization

If presented with a Chip & PIN card, the card must be inserted into the chip-reading terminal and the terminal prompts should be followed.

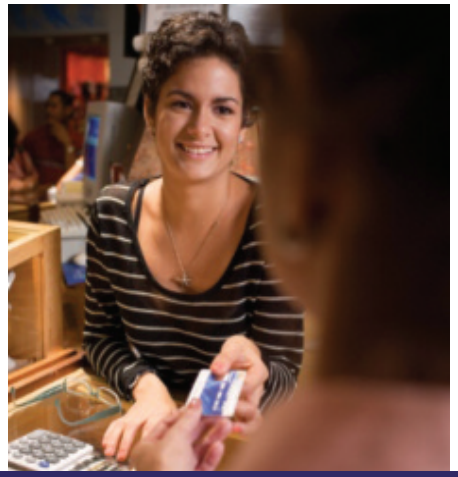
If card is PIN-preferring, the cardholder will be required to enter a PIN.

Even if the transaction is pre-authorized - when checking into a hotel or renting a car, the credit card will need to be presented on arrival and the customer will be asked to enter their PIN to accept the estimated amount.

Estimated Authorization

When the customer arrives, you may estimate the total charges and obtain an authorization for the estimated amount. This estimate of the guest's total charges should be based on:

- **Hotels:**
  - Expected length of stay
  - Room rate including tax
  - Incidental charges such as room service, telephone calls, and parking
- **Car Rental:**
  - Expected length of rental.
  - Applicable daily, weekly, monthly rental rate (including tax).
  - Incidental charges such as insurance, and any other additional necessities.
  - Mileage rates
  - Never overestimate or pad the authorization amount
  - Never require a customer to sign a blank draft or a deposit receipt for damages.



4

Final Authorization

When the guest checks out or car is returned, authorization is required in the following instances:

- If there was no previously estimated authorization and the actual transaction amount is above your floor limit, authorize the actual transaction amount.
- The final settlement amount must be within 15 or 20 percent of the authorized amount. (15% Visa and MC or 20% Discover)
- Car Rentals paid with Visa, the final settlement amount must be within 15% or US $75, whichever is the greater of the authorized amount. Incremental authorization is not required if the settlement amount falls within the allowed tolerance
- If there was a previously estimated authorization amount, apply the "15% or 20% rule" or Visa US $75 for car rentals, to determine whether or not an incremental authorization is required.
  - Add 15% or 20% or Visa US $75 for car rentals, to the previously estimated authorization amount.
  - Compare the total to the actual (or final) transaction amount.
  - If the actual transaction amount is more than the sum of the previously estimated authorization amount plus 15% or 20% or Visa US $75 for car rentals, an incremental authorization is required for the difference between the previously estimated authorization amount and the actual transaction amount.
- Authorization remains valid for the estimated length of a guest's stay or customer's car rental. If beyond the original estimate of the length of the customer's hotel stay or car rental, you should obtain an incremental authorization approval for the additional transaction amount that you expect will be generated during the extended period.
- If a hotel stay or car rental extends beyond 2 weeks, you should settle the transaction and obtain authorization for a new transaction.

Delayed or Amended Charges

A delayed or amended charge may include room, food, or beverage charges, taxes, mileage charges, fuel, insurance, rental fees, and parking tickets and other traffic violations and must not include charges for loss, theft, or damage.

A delayed or amended charge must be processed to the Cardholder's account within 90 calendar days of the Transaction Date of the related Transaction.

Damages

- Card Plan Regulations prohibit the application delayed or amended charges if the charge represents loss, theft or damage. However, a merchant may charge a separate "non-delayed and amended transaction" for damages if the cardholder agrees to that transaction.

  If the cardholder agrees to pay for the damages, the merchant may charge for damages consented to by the cardholder.
- Charges for damages must be processed as a separate transaction. The merchant must provide a reasonable estimate of the cost to repair the damages and obtain agreement from the cardholder. If the cardholder chooses to pay for the repairs, the merchant must:
  - Prepare a specific sales slip with proof of card presence via Chip or Swipe.
  - Provide the estimated amount for repairs indicating that the amount will be adjusted accordingly pursuant to completion of the repairs and submission of the invoice for such repairs.
  - Obtain PIN verification or signature from the cardholder.

Note: *A merchant is not permitted to require a cardholder to sign a blank transaction receipt. If such actions are taken by a merchant, the issuer may pursue compliance.*

Refund Limits & Purchase Corrections

Not all fraud threats are external. Some of the most significant threats can be posed by bad employees. The risk of employee fraud comes from the ability to refund on either a debit or credit card.

Refunds

- A refund is the process followed to reimburse a cardholder when they have returned an item or cancelled a service that was to be provided.

Purchase Correction

- A purchase correction is the means to correct an error. An example would be when a merchant bills a cardholder $1000.00 when the correct amount was $100.00.

It is important to follow the proper procedures as each function has unique financial limits and there are risks to both the merchant and Moneris when terminal functionality is misused.

We recommend a $0.00 debit refund limit (exchange only, cash refunds, in-store credit)

Unlike credit refunds, debit refunds are immediately posted to the cardholder's bank account. And the debit refund limit is a per transaction limit.

Best Practices for client refund processing

- Restrict access to your POS equipment;
- The authority to process refunds should be restricted to one or two people at a supervisory level (on certain POS devices);
- Implement pass codes and put processes in place to safeguard such pass codes
- Daily audits should be performed on refunds (to match refunds to sales).

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.

5

Unembossed and Prepaid Cards

Unembossed and Prepaid Cards are similar to the cards you currently accept. They may take the form of a credit, debit, or prepaid/gift card, and will have the same familiar brand mark such as Visa, MasterCard and Discover.

Unembossed cards

One major difference with unembossed cards is that the card will look "flat". All account information – cardholder name, primary account number (PAN), validity date, and security character – is projected onto the front of the card with tamper-evident laser engraving or indent printing rather than embossing. "Electronic Use Only" must be printed on the front of the card.

Unembossed cards can only be used in electronic terminals that are capable of online authorization. They cannot be key-entered. If a POS terminal is not available, merchant should advise the customer to contact the Card Issuer or request for another form of payment. If an Unembossed Card is manually key-entered, merchants will be liable for any chargebacks.

Prepaid Cards

Visa, MasterCard & Discover Prepaid cards can be embossed, with raised characters, or unembossed, meaning they're flat and smooth. On unembossed cards, you'll see the words ELECTRONIC USE ONLY, which means transactions should be processed at an electronic terminal that allows for automatic authorization. Prepaid cards can be personalized with the cardholder's name
or they may be non-personalized – both types of card are processed the same way.

Prepaid cards can be used anywhere that accepts Visa, MasterCard or Discover, including mail order, online and point of sale retail merchants. Prepaid cards must be registered before making online purchases; cardholders can do this with the card Issuer via the Internet or over the phone.

A cardholder returning an item must present the prepaid card used to make the purchase along with the original sales receipt.

6

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.

- 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 or decline the transaction
- 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.

Protecting your business

Even when proper procedures are followed there are no guarantees that it is a legitimate transaction. If there is any suspicion of fraud, initiate a Code 10 authorization or decline the transaction

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 and hold the card in your hand during the authorization process.
- Stay calm and remain casual and courteous with the customer.
- Your call will be transferred to the Card Issuer who is able to validate the information. 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.

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

Mail/Telephone Order and Internet Fraud

Card Not Present:

A transaction that occurs when the card, the cardholder, or the merchant representative is not present at the time of the transaction (such as but not limited to mail order, telephone order, or Internet transactions).

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 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 (funds) are available and that the card is not currently blocked. To detect fraud, authorizations must be augmented with the right combination of tools and controls.

To process a Card absent transaction, manually key enter the card number. Ensure that the expiry date and the amount are entered and verify the authorization response.

If merchandise is to be shipped, an authorization for Mail/Phone Order or Electronic Commerce transaction can be obtained up to 7 calendar days of the transaction date. For such a transaction the transaction date is the date the merchandise is shipped.

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 the front of the card
- Separately confirm the order by sending a note via the customer's billing address, rather than the "ship to" address.
- Develop processes whereby orders can be pended for further review before fulfilling the request
- Diligence and monitoring must be applied to adequately review your transactions
- If you suspect fraud contact the card issuer to advise them of your suspicions.

Moto/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
- **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.

Fraud Prevention Tools

Verified by Visa & MasterCard SecureCode

Merchants are open for chargebacks with card absent processing. Any disputes will be returned, regardless of what was verified or investigated.

The only exceptions are the *Verified by Visa* and the *MasterCard SecureCode* programs.

Merchants must register and be approved for *Verified by Visa* or *MasterCard SecureCode*. The objective of these programs 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 or *MasterCard SecureCode* 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.

Verified by VISA

MasterCard SecureCode

AVS – Address Verification Service

- AVS provides merchants with a method to verify the billing address given by the cardholder, to the billing address on file with the credit card issuing bank.
- Participating cards: Visa, MasterCard and Discover®, all with similar features.
- It is important to note that AVS is only a tool and is most effective when used in conjunction with other fraud tools and risk indicators.
- Regardless of the AVS result, if the card Issuer does not approve the authorization request, do not complete the transaction.

AVS alone will not prevent a Fraud related Chargeback

CVD – Card Validation Digit (CVV2, CVC2, CID)

- CVD is a 3 digit code printed in the signature panel of Visa, MasterCard and Discover issued cards and 4 digit code printed on the front of American Express® cards.
- This code helps to ensure that the customer making the Mail Order/Telephone Order or eCommerce transaction is in possession of his or her credit card.
- Be vigilant if the customer cannot provide the CVD code or the code does not match to that on file with the Issuer, it's more than likely that the card is not present and the number given could be stolen. In the case of an unmatched code, ask the customer to confirm it and if it still does not match, further validate or decline the transaction.
- Regardless of the 3 or 4 digit code verification response, if the card Issuer does not approve the authorization request, do not complete the transaction.

CVD alone will not prevent a Fraud related Chargeback

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.
- Follow PCI Standards to keep your systems secure

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?

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

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.

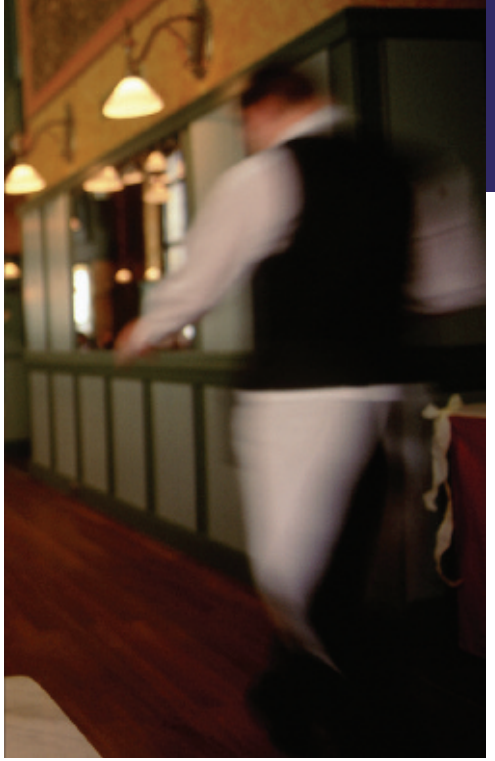
For debit cards

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.



"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."

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: *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.

Moneris Solutions 24/7/365 Customer Service
Phone: 1-866-319-7450

Credit Card IVR Authorizations and Code 10
Phone: 1-866-802-2637