Merchant Operating Manual

Moneris SOLUTIONS

Moneris Solutions Corporation ("Moneris") is Canada's leading provider of debit and credit card payments processing. For businesses accepting card payments from cardholders, Moneris offers merchants a "single point of contact" for VISA®, MasterCard®, Interac®, Discover®, UnionPay and American Express®, and all Point of Sale (POS) equipment, machines, and solutions – from in-store pin pads and POS terminals to mobile wireless to e-commerce.

Processing Transactions

Merchant Identification and Responsibility for Transactions

You must ensure that you prominently and unequivocally inform the cardholder of the identity of you the merchant at all points of interaction, so that the cardholder readily can distinguish you the merchant from any other party, such as a supplier of products or services to you the merchant.

You must ensure that the cardholder understands that you the merchant are responsible for the transaction, including delivery of the products (whether physical or digital) or provision of the services that are the subject of the transaction, and for customer service and dispute resolution, all in accordance with the terms applicable to the transaction.

Valid Transactions

You must submit valid transactions only between you and a bonafide cardholder. You must not submit transactions that you know or should have known are fraudulent or not authorized by the cardholder, or authorized by a cardholder colluding with you the merchant for a fraudulent purpose. You are deemed to be responsible for the actions of your employees, agents, representatives and any other person that processes transactions.

Discrimination

You must not engage in any acceptance practice that discriminates against or discourages the use of a card in favour of any other particular card brand.

Remember the Basics

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

- Look for the hologram, the printed bank identification number, the unique embossed symbol and the signature panel.
- Check the card expiration date.
- If you use a POS terminal to authorize credit card transactions, use it to read the information on the card by swiping or inserting (with a PIN) into the POS terminal.
- If you are satisfied that the card is genuine, use the appropriate authorization procedures to request authorization.

For a chip card transaction, please see the *How it Works* section (page 4) within this operating manual.

- If it is a magnetic stripe transaction, have the cardholder sign the draft in full view.
- Compare the signature on the card with the signature on the receipt to ensure they match.

Proper Processing Procedures

CHIP CARDS

A chip card is a debit or credit card with an embedded microchip that the cardholder inserts into a POS terminal card reader or ABM. Instead of a signature, the cardholder enters a PIN to authorize the transaction. Because chip cards process data securely, it is difficult to copy or tamper with them. The PIN feature provides added security as well as addressing concerns among Canadian merchants regarding the cost of fraudulent card activity.

Chip Technology helps to:

- Reduce chargebacks
- Reduce fraud
- Simplify store operations
- Increase POS checkout speed

HOW IT WORKS

A transaction using a chip & PIN card with a chip-reading POS terminal is simple. Rather than swiping the card and signing a receipt, cardholders insert their chip & PIN card and enter their PIN into a chip-reading POS terminal to verify their identity. UnionPay transactions require a cardholder signature for all transactions including PIN verified; you may not be protected from chargebacks if you do not obtain the cardholder's signature.

Important things to know about chip & PIN Cards

- If you observe that the card presented has a chip, it should be inserted into the POS terminal.
- When presented with a chip card, do not swipe the card first. Simply insert the card and follow the prompts.
- We recommend that you do not key enter a chip card transaction on your chip device. Key-entered transactions may not be protected from chargebacks, even if you obtain an imprint, an authorization and a signature. Manual key-entered transactions are not permitted for transactions processed with a UnionPay card unless you are a hotel or car rental merchant and are processing a hotel or car rental reservation pre-authorization transaction.
- With chip & PIN cards, the cardholder will be prompted to enter a PIN. In some chip cards, a signature is required when prompted by the terminal. UnionPay transactions always require a cardholder signature on all transactions.
- A chip card must remain inserted in the POS terminal for the duration of the transaction. Do not remove the card until the POS terminal prompts you to do so. Removing the card before the transaction is complete will cancel the transaction.
- As a best practice, we recommend that you look at the bottom of the receipt and circle the text "VERIFIED BY PIN". UnionPay receipts do not display the text "VERIFIED BY PIN".

IMPORTANT:

Leave the chip & PIN card in the reader for the duration of the transaction.

1. Begin the purchase transaction.
2. Check for the chip on the card.
3. Insert the chip & PIN card when prompted. Insert card, chip side up.
4. Follow the prompts.
5. Wait for the "Remove card" message then remove the chip & PIN card.

The transaction is complete!

Swiping a Card

- Before swiping, make sure the magnetic stripe is facing the reader.
- Always swipe the card once in the direction 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 magnetic stripe.
- If you receive a message of "**Call**" or "**Call Centre**" on your POS terminal, call the authorization number at **1-866-802-2637**.
- If you suspect fraudulent activity, or have any questions regarding transaction authorization, ask for a Code 10 authorization.
- If the authorization centre requests that you retain a card, do so only by reasonable and peaceful means. Never put yourself in danger.

Manual Transactions

If you use a POS terminal to process transactions, your floor limit is zero and you must obtain an authorization number for each transaction. Manual key-entered transactions are not permitted for UnionPay unless it is to process a hotel or car rental reservation pre-authorization transaction.

IMPORTANT NOTE:

- It is important to remember that an authorization does not mean that the actual cardholder is making the 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 help detect and prevent fraud, authorizations should be augmented with the combination of tools and controls.

- The chip and magnetic stripe are active components of the card's security that make manual processing appropriate only when a card's magnetic stripe can't be read.
- **When a card's chip or magnetic stripe cannot 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
  - Total dollar value of transaction, including taxes and other charges
  - Cardholder signature
  - Authorization number
  - Merchant name and number
  - Do not write "void" or "copy" on the face of the manual sales draft
- **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

TIP:

When a card's chip or magnetic stripe cannot be read, it's usually because:

- the chip or magnetic stripe reader is broken or dirty
- the reader is obstructed, preventing a clean insert or swipe
- the card was inserted or swiped improperly
- the card's chip or magnetic stripe is damaged

IMPORTANT INFO:

It's a good idea to monitor your rate regularly. Moneris offers online statement and reporting services through Merchant Direct®. With this tool you can view your credit and debit card transactions online. Information is updated daily, which is ideal for balancing and monitoring cash flow and you can also import this data into spreadsheets for forecasting and trend analysis purposes. It also allows you to send and receive online customer service inquiries. An online demo can be viewed at moneris.com/merchantdirect or for more information you can contact the Moneris Sales Centre at 1-866-666-3747 (1-866-MONERIS).

Key Entry

We recommend that you do not key enter a transaction on your device. Key-entered transactions may not be protected from chargebacks, even if you obtain an imprint, an authorization and a signature. Manual key-entered transactions are not permitted for UnionPay unless it is to process a hotel or car rental reservation.

Key-entered (as opposed to chip-verified or card-swiped) transactions have some real disadvantages including, but not limited to:

- An increased risk of fraud and/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 the POS terminal.
- 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.

If a transaction is key-entered, you must 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 some chargebacks.

For authorizations, the transaction must be authorized 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.

Steps to Minimize Key Entry

- Regularly check the chip and magnetic stripe reader on the POS terminal to be sure it is working properly.
- Clean readers periodically with the reader cleaning card that came with your POS terminal. To order cleaning cards and other supplies for your business from Moneris please visit us online at shopmoneris.com or call us at 1-866-319-7450.
- Position readers to facilitate a full insert or card swipe with any obstructions removed.
- Do not allow staff to place items near readers that could soil or damage the POS equipment, particularly food and beverages.
- Do not place readers near any equipment that deactivates magnetic anti-theft devices attached to merchandise.

Help Cardholders "Protect Their PIN"

Cardholders need to be able to enter their Personal Identification Number (PIN) without the PIN being seen by others.

Ensure the POS terminal is installed so that the cardholder can easily shield the PINpad with their body or that privacy shields are installed if your PINpad is immovable and/or mounted in a stand.

Allow the cardholder to hold the PINpad until they receive the final authorization/decline response message.

Always give the cardholder a copy of the transaction record and return their card to them.

Downtime Procedures

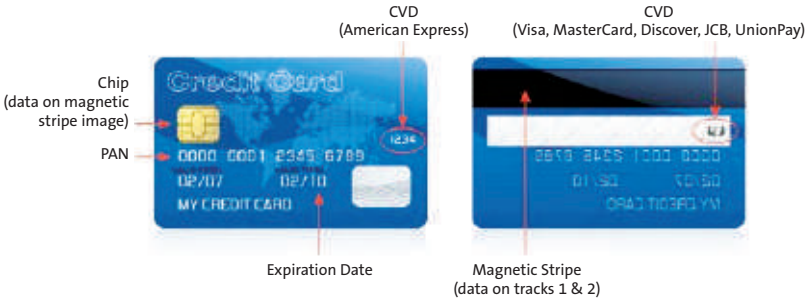
If you are experiencing system failure, the following procedures must be followed when accepting credit cards except for UnionPay; you cannot accept UnionPay cards when the system is down:

- Take a manual imprint.
- Phone for voice authorization and record the authorization number on the manual sales draft. Call **1-866-802-2637**.
- Have the cardholder sign the imprinted copy.
- When system/service is restored, force post the transaction on your electronic POS terminal using the assigned authorization number.
- Please ensure that all of the information is clearly visible on the manual sales draft.
- Please see the section on *Manual Transactions* within this operating manual for the information required on a sales draft.

Protecting Your Business Against Fraud

How to Identify Security Features

Types of Data on a Payment Card



Suspicious Customer Behaviour

Be alert and observe your customers.
Detecting credit card fraud 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 may display one or more of 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 about to close.
- 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 cardholder may take the card from their pocket instead of a wallet or purse.
- The cardholder may sign the sales draft in a deliberate and/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 cardholder may randomly charge expensive items on a newly issued card.

COUNTERFEIT CARDS

Confidence

- The cardholder may look the part of someone who purchases expensive items. They may be well-dressed and self-confident.
- They are confident that their purchases will be authorized given they are involved in the production of these high quality cards.
- They may spend a lot of time browsing and may pick up merchandise the following day.

Come back for more

- The cardholder may return with friends, who will 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 the best guide.
- If you or your staff have any doubts or suspicions, give yourself, not the cardholder, the benefit of the doubt. Call for a Code 10 authorization (see *Procedures for Lost/Stolen/Forgotten Cards*) which is used when you suspect a card transaction may be fraudulent or suspicious.

Procedures for Lost/Stolen/Forgotten Cards

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 for payment.

PROTECTING YOUR BUSINESS

Even when proper procedures are followed, 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 authorization:

- 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.
- Keep possession of the card during the authorization process. Stay calm and remain casual and courteous with the cardholder.
- 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.

Forgotten Cards

If a card is left at your location:

- Return the card to the cardholder if reclaimed within 24 hours with proper identification.
- If it is not reclaimed within 24 hours, cut the card in two pieces and return all cards to the address set out below:

Moneris Solutions
Attn: Merchant Rewards
PO Box 219 Stn D
Toronto, ON M6P 3J8

Please ensure that you include the below information when returning the card:

- Store name
- Address
- Name of the person who retained card
- Phone number
- Attention: Merchant Rewards

Please also note that rewards are at the discretion of the card issuer.

Suspected Skimming

Skimming is the transfer of electronic data using a card reader, from one magnetic stripe to another for fraudulent purposes. 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 that can be used to skim magnetic stripe information from credit and debit cards through either a tampered or dummy POS terminal.

BE ALERT

- There are now portable skimming devices that capture card track data.
- These devices have the capacity to run for long periods of time as they can have a larger storage capacity.
- Check under the counter which can be a convenient hiding spot for skimming devices and activity.

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" i.e. looking over a cardholder's shoulder to view the PIN number being entered– either the employee or an accomplice will "surf" at the moment the cardholder enters his/her PIN into the PINpad.
- Using a mini-camera lens to capture the PIN number.
  The camera is placed either in a hole in the ceiling or on a shelf above the counter and the PINpad. With this type of equipment, the PINpad needs to remain in a fixed position on the counter in order for the lens to capture the numbers being keyed in by the cardholder.

For more information on skimming, please visit moneris.com.

Mail/Telephone Order and E-commerce Fraud

Many of the safeguards against fraud in traditional retail environments are not applicable in environments where a card is not present at the time of the transaction, including mail/telephone orders (MOTO) and e-commerce orders. These transactions do not require face-to-face contact or an actual card in hand, so there is anonymity associated with the transaction.

All MOTO and E-commerce merchants are required to authorize their transactions.

If funds are available and a card has not been reported lost or stolen, the transaction will most likely be authorized by the card issuer.

It is important to remember that an authorization does not mean that the actual cardholder is making the purchase or that a legitimate card is involved. An authorization only means that credit is available and that the card is not currently blocked.

Best Practices to help reduce E-commerce Fraud

- Authorize all transactions regardless of the dollar amount.
- Implement the applicable fraud prevention tools (AVS, CVD, VbV, Secure Code).
- Only charge the cardholder for merchandise that has been shipped.
- Credit the cardholder's account immediately if they have returned the merchandise or are disputing the charge.
- Whenever possible, ship products with a courier that obtains signatures as proof of delivery.
- Keep detailed records of all order forms, shipment slips, delivery receipts, and information such as address, telephone number, signature, pertinent invoices, and e-mail address.
- Develop and maintain a cardholder database or account history files to track buying patterns and compare individual sales for signs of possible fraud.
- Track "problem" credit card accounts (i.e. accounts that have had chargebacks in the past) and cross-reference on future orders.
- Track IP addresses.
- Establish and enforce appropriate controls on the employees who have access to the cardholder database and account numbers.
- Follow Payment Card Industry Data Security Standards (PCI DSS) to keep your systems secure (see the section on *PCI DSS* within this operating manual).

IF YOU SUSPECT FRAUD

If you are suspicious of a transaction or find the circumstances of a transaction questionable, ask the cardholder to provide additional information such as:

- their day and evening telephone numbers, which can be verified through Directory Assistance or **canada411.ca**.
- the bank name on front of their card or you could;
  - Call in for a name & address verification (see *Address Verification Service (AVS)* under the E-commerce section).
  - If still suspicious, do not proceed with the sale.

Chargebacks

Overview

A Chargeback occurs when a credit or a payment for which an authorization may have been provided is reversed.

It may result from a cardholder dispute, or when proper acceptance or authorization procedures were not followed. These adjustments are processed to your account automatically and are accompanied by an adjustment advice and a chargeback summary report sent to you either by fax or mail or online through Merchant Direct Secure Message Centre.

In some cases, chargebacks can be reversed if you supply proper documentation within the strict specified timeframes set out in your merchant agreement. If you receive a chargeback adjustment advice, it is recommended that you respond to it immediately.

The adjustment advice is accompanied with clear instructions on what information you will need to supply in order to refute the chargeback. If you need assistance or information pertaining to a chargeback, please don't hesitate to contact **Merchant Customer Service at 1-866-319-7450**.

A list of some of the more common chargeback reason codes for which your account could be adjusted are available online at moneris.com/chargeback.

Please take a moment to read through the codes and familiarize yourself with the important tips that may help you to avoid chargebacks.

Retrieval Requests

From time to time, you may be asked by the card issuer to supply a copy of a sales draft or transaction record for a sale completed at your place of business. These requests are generally initiated by cardholders who need verification or clarification of charges made to their credit or debit card account, or from other payment card issuing financial institutions to satisfy some fraud or dispute situations.

As a merchant accepting payment cards, you are required to retain copies of all sales/transaction receipts/drafts for a minimum of 18 months from the transaction date and respond to the request within the timeframe in your merchant agreement.

If you receive a Retrieval Request from Moneris Solutions, respond to it immediately by sending a legible copy of the document that was used to bill the transaction to the cardholder's account. Examples of these documents are manual sales drafts, POS terminal transaction receipts, invoices, folios, car rental agreements, purchase order forms, etc.

The document must include the following requirements:

- Truncated Card number
- Authorization number
- Cardholder name
- Cardholder signature (if applicable)
- Merchant name
- Merchant location
- Transaction date
- Transaction amount
- Or any other document as requested
- Please also include the original retrieval request

IMPORTANT NOTE:

- If you receive a retrieval request on an item where you already processed a refund, please send Moneris all applicable documentation regarding this refund as well.

FAX ALL DOCUMENTATION TO:

For Retrieval Requests:
416-231-9329 (Local) or
1-866-596-1116 (Toll free)

For Chargeback Requests:
416-734-1561 (Local) or
1-866-354-3797 (Toll free)

Retain your Fax Confirmation Report as your proof of fulfilling the retrieval/chargeback request.

RESPONSES MAY BE SENT BY MAIL TO:

Moneris Solutions
P.O. Box 410 Station "A" Toronto, Ontario M5W 1C2

MERCHANT DIRECT

Documentation may be viewed online through Merchant Direct Secure Message Centre. If you are not currently registered for Merchant Direct, please contact Merchant Customer Service at **1-866-319-7450** or visit **moneris.com/merchantdirect**.

Timeframes are critical! Failure to supply a copy of the requested transaction information within the specified timeframe in your merchant agreement could result in a non-reversible chargeback. To ensure you receive retrieval requests and chargeback notifications, please ensure your merchant location mailing address, fax and phone numbers are regularly updated.

Please ensure that you are thorough in supplying the appropriate documentation to Moneris to satisfy the applicable chargeback reason codes.

USEFUL TIPS ON CHARGEBACKS AND RETRIEVALS REQUESTS

- To help avoid confusion for the cardholder with the transaction, ensure your deposits are settled daily.
- To avoid confusion with the merchant description on the cardholder statement, ensure the business name printed on the sales draft matches the name on your store front or for online transactions the name matches your website information.
- If you discover that a transaction has been duplicated, process an immediate credit to the cardholder's account.

- If you are asked to supply a sales draft for a card that originally could not be inserted or swiped in your POS terminal, be sure to provide the manual sales draft to confirm that a card imprint was taken and that the card was present in your establishment at the time of the sale.
- To help avoid a potential non-reversible chargeback to your account, ensure that the retrieval timeframes are strictly followed and that your responses are promptly sent.
- Respond to all retrieval requests, even if they appear to be duplicates.
- Always respond to retrievals and chargebacks with legible copies of the transaction information document.

For any assistance with retrieval requests or chargebacks, or if you would like to receive them by fax or Merchant Direct, please contact Merchant Customer Service at 1-866-319-7450.

Chargeback Reason Codes

VISA/MASTERCARD/DISCOVER/UNIONPAY

A list of all the chargeback reason codes for which your account could be adjusted are available online at moneris.com/chargeback.

Best Practices

- Ensure that all face-to-face transactions are authorized through your POS terminal; the card must be inserted with a PIN or swiped with a signature as the card verification method.
- For a card present sale, if the card presented cannot be inserted or swiped through the POS, a manual imprint must be obtained using an imprinter. Ensure the transaction is authorized and the receipt is signed. Manual key-entered transactions are not permitted for UnionPay cards unless it is to process a hotel or car rental reservation pre-authorization transaction.
- Obtain proper authorization (with full transaction amount, appropriate valid and expiry dates) for all transactions, on the date of the transaction.
- Do not process transactions for which "Declined" authorization responses are received. Ask for another means of payment.
- Ensure that all accepted cards include logo and security features.
- For UnionPay, a 15 percent variance is allowed to restaurants for gratuity purposes only. Therefore the actual (or final) amount must not exceed 15 percent from the authorization amount.
- For Visa, MasterCard and Discover, a 20 percent variance is allowed to restaurants for gratuity purposes only. Therefore the actual (or final) amount must not exceed 20 percent from the authorization amount.
- Ensure that all written characterizations or description of goods and/or services for non face-to-face transactions are detailed, accurate and not misleading.
- Ensure that all merchandise shipped is received by and signed for by the cardholder. When possible, obtain an imprint of the card at the time of delivery. Have the cardholder confirm delivery by signing the shipping invoice.
- Ensure that all merchandise shipped is suitable for the purpose for which it was sold and delivered in a satisfactory condition.
- Ensure your return, refund and cancellation policies are clearly outlined at the time of the transaction. Failure to disclose your refund or return policy can result in a dispute if your customer returns the merchandise.
- For 'recurring' transactions that are billed periodically (monthly, quarterly or annually), if the cardholder requests cancellation you should cancel the transaction as specified by the customer and in accordance with your agreement with the customer.
- For a delayed delivery transaction, the customer should only be billed when the merchandise has been shipped.
- Have the cardholder sign an agreement or contract for any services to be provided or merchandise to be delivered.
- Ensure that all services are provided within the contracted timeframes. Services paid for by "other means" should not be billed to the cardholder's card.
- Avoid processing a single transaction more than once; reconcile your daily deposits to ensure the transactions are processed correctly. Should you discover a duplicated transaction, we recommend that you immediately process a refund to the cardholder's account and promptly advise the cardholder about the refund to avoid a chargeback.
- Ensure that all electronic deposits (sales and refunds) are settled via your POS terminal within three business days from the date of the transaction.
- Ensure that all refunds are entered as a credit/refund and not as a sale via a POS terminal.
- 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.

Card Brand Programs

RISK PROGRAMS

The card brands monitor chargeback and fraud levels of all merchants accepting their cards. Merchants are required to keep their chargeback and fraud rates below specific thresholds and, whenever excessive chargeback or fraud levels are detected, merchants will be required to take corrective action.

The corrective action a merchant may be required to take will depend on certain factors, including but not limited to merchant type, the merchant's sales volume, and its geographic location. Often merchants need to provide their sales staff with additional training on card acceptance procedures. Merchants may also be required to develop a detailed chargeback/fraud-reduction plan.

The programs include:

VISA PROGRAMS

Merchant Fraud Performance Program (MFPP)

This program consists of thresholds for merchant fraud performance, and a compliance framework to ensure timely resolution to adequately reduce fraud levels.

The program consists of two components, one that addresses local market fraud performance and one that addresses inter-regional/ cross-border fraud performance.

The local market fraud component measures domestic fraud against sales activity and identifies merchants that do not meet the Visa Canada performance threshold(s). Merchants have a specific period of time in which to address performance issues, after which, fines may be applied.

The inter-regional / cross-border fraud component measures fraud against sales activity between Visa regions and identifies merchants that do not meet the Visa Canada performance threshold(s).

The inter-regional / cross-border fraud component consists of two performance measurements:

- **Minimum fraud performance threshold**.
  This threshold is designed to ensure the timely resolution of issues that routinely arise as a consequence of sub-standard inter-regional/cross-border fraud control and acceptance practices.
- **Excessive fraud performance threshold**.
  This threshold will implement immediate action against merchants that present a high inter-regional fraud risk to issuers based on Visa's performance standard threshold.

Merchants have a specific period of time to address performance issues, after which chargeback liability and fines may be applied.

Global Merchant Chargeback Monitoring Program (GMCMP)

Visa monitors international transactions to identify merchants that generate excessive chargebacks (in relation to international card transactions).

Merchants have a specific period of time to address performance issues, after which chargeback liability and fines may be applied.

MASTERCARD PROGRAMS

Global Merchant Audit Program (GMAP)

The Global Merchant Audit Program (GMAP) is a fraud monitoring and management program that identifies merchants that exceed an acceptable level of fraud in any one month based on an established set of program criteria.

Merchants have a specific period of time to address performance issues, after which chargeback liability and fines may be applied.

Excessive Chargeback Program (ECP)

The Excessive Chargeback Program (ECP) is designed to closely monitor, on an ongoing basis, chargeback performance at the merchant level and to promptly determine when a merchant has exceeded or is likely to exceed monthly chargeback thresholds.

The "chargeback-to-transaction ratio" or "CTR" is the number of MasterCard chargebacks received by a merchant in any given calendar month divided by the number of MasterCard sales transactions in the preceding month.

UNIONPAY PROGRAMS

High-Risk Merchant Monitoring Program (HMMP)

The High-Risk Merchant Monitoring Program (HMMP) is a fraud monitoring and management program that identifies merchants that exceed an acceptable level of fraud based on an established set of program criteria.

Merchants have a specific period of time to address performance issues, after which chargeback liability and fines may be applied.

Merchant Chargeback Monitoring Program (MCMP)

The Merchant Chargeback Monitoring Program (MCMP) measures chargebacks relative to merchant sales. The program monitors chargebacks to ensure a merchant's chargeback to transaction ratio is not excessive.

Merchants have a specific period of time to address performance issues, after which chargeback liability and fines may be applied.

DISCOVER PROGRAM

The Discover excessive chargeback program is designed to monitor chargeback and refund performance and ensure a merchant's chargeback to transaction ratio is not excessive for a given month.

IMPORTANT NOTE:

- Each Visa, MasterCard, Discover and UnionPay monitoring program listed is subject to a different fine or fee and assessment structure.
- These programs are subject to change from time to time, including changes in monitoring criteria and thresholds.

For more details on the risk programs, including compliance thresholds and possible fines for non-compliance, please visit moneris.com.

Other Programs

VISA EASY PAYMENT SERVICE (VEPS)

VEPS enables qualifying merchants to process Visa transactions less than or equal to $25.00 CAD (including tips and taxes) quickly and conveniently; plus you are protected from certain chargebacks for those transactions that qualify for the program. In the VEPS program:

- Card is swiped and transaction is authorized.
- No cardholder signature is required.
- Cardholder receipt is only provided upon request.

VEPS Eligible Transactions

To qualify for the VEPS program, a transaction must have the following characteristics:

- The transaction is properly identified and the total transaction value is less than or equal to $25.00 CAD (including tips and taxes).
- Conducted in the Face-to-Face environment.
- Card account data must be swiped.
- Fully Authorized.
- For magnetic stripe transactions only; not applicable to chip cards.

Any transaction which does not meet all of the above requirements does not qualify as a VEPS Transaction. Transactions which are key-entered or made at Unattended Acceptance Terminals are not VEPS Transactions and are subject to all requirements of the Visa Operating Regulations.

For more information on VEPS, visit visa.ca.

DISCOVER NO SIGNATURE REQUIRED (NSR)

Discover transactions less than or equal to $50.00 CAD (including tips and taxes) are eligible for treatment in Discover's NSR Program. For faster service, the NSR Program allows merchants to process a Discover transaction without having to obtain a signature on the receipt or provide a receipt to customers. You must however provide a receipt at the cardholder's request.

To qualify for the NSR program, a transaction must have the following characteristics:

- The transaction is properly identified and the total transaction value is less than or equal to $50.00 CAD (including tips and taxes).
- Card is swiped and transaction is authorized.
- No cardholder signature is required.
- Cardholder receipt is only provided upon request.
- Card Sale took place in a Card Present Environment.
- For magnetic stripe transactions only; not applicable to chip cards.

For more information on Discover's No Signature Required program, visit discover.com.

CONTACTLESS PROGRAMS

Contactless payment programs are designed to speed up checkout and simplify the payment process. Instead of swiping or inserting the card in a terminal, the customer waves or taps it on a special contactless reader. No signature or PIN is required for transactions under a specified amount (see below for program details). You do not need to provide a transaction receipt to the cardholder unless the cardholder specifically requests one or if the transaction is above the prescribed limits. You are still required to keep a copy of the receipt for your records in case of a dispute.

To enable these programs you will need a certified contactless reader and contactless capable point-of-sale terminal or software system. Only transactions processed through a certified contactless reader qualify for these programs.

MasterCard PayPass

The MasterCard PayPass Contactless program applies to transactions less than or equal to $100.00 CAD (including tips and taxes).

MasterCard transactions over $100.00 CAD (including tips and taxes) should be processed using another point-of-sale payment method, such as swiping or inserting the card. If the contactless reader is used for transactions over $100.00 CAD, chargeback protection will no longer apply and you will be liable for the full transaction amount.

Visa payWave

The Visa EPS Contactless program applies to transactions less than or equal to $100.00 CAD (including tips and taxes). Cardholder's signature will be required for credit card transactions over $100.00 CAD.

Discover ZIP

The Discover ZIP Contactless program applies to transactions less than or equal to $50.00 CAD (including tips and taxes). Cardholder signature will be required for transactions over $50.00 CAD.

Interac Flash

The Interac Flash Contactless program applies to transactions less than or equal to $100.00 CAD (including tips and taxes). If the transaction is above the set dollar limit, you will be asked to insert the card and enter a PIN to conduct a chip debit transaction.

For more information, please visit moneris.com/quickservice.

Card Acceptance Standards

Primary Account Number (PAN) Truncation (card masking)

The Primary Account Number (PAN) appears on electronically generated transaction receipts and must be masked.

Cardholder Copy

All but the last four positions of the PAN must be disguised or suppressed and, if applicable, the expiry date be suppressed on the cardholder copy of the transaction receipt.

- **Interac advises** that an abbreviated version of the PAN may be used provided it is sufficient to identify the specific card used to initiate the transaction.

Merchant Copy

Display only a maximum of the first six (6) and last four (4) positions of the PAN on the merchant copy of the transaction receipt while disguising the rest and suppressing the expiration date.

The card brands require that the masked portion of the PAN must be replaced with fill characters that are neither blank spaces nor numeric characters, such as 'x', '*', or '#'.

Prepaid Cards

Prepaid Visa, MasterCard, Discover and UnionPay cards are payment cards containing a preset amount of funds that can be used at any merchant location that currently accepts credit cards for purchases.

Processing a prepaid card transaction:

- Ask the cardholder how much to deduct.
- Follow the same procedures as you would with a credit card – swipe the card, enter the amount and obtain an online authorization.
- Ask the cardholder to sign the receipt and check the signature against the one on the card.
- A prepaid card can only be used at POS terminals that can obtain an immediate online authorization.

For more information on prepaid cards visit moneris.com

mastercard.com

visa.ca

discover.com

Surcharging/Convenience Fees

You must not add any surcharges/convenience fees to any transactions unless otherwise permitted in accordance with card brand rules and regulations.

Minimum/Maximum Transaction Amount Prohibited

You are not permitted to set a minimum or maximum transaction amount to accept a valid and properly presented card.

Prohibited Transactions

A prohibited transaction means a transaction carried out by you or in furtherance of a prohibited or illegal activity, transactions Moneris advises you from time to time are prohibited transactions, or any other transactions that you are not authorized to process.

You must not submit for payment into interchange, including but not limited to any transaction that:

- Represents the refinancing or transfer of an existing cardholder obligation that is uncollectible, or
- Arises from the dishonour of a cardholder's personal cheque, or
- Arises from the acceptance of a card at a POS terminal that dispenses scrip.

Illegal or Brand-damaging Transactions

You must not accept card payment for any transaction that is illegal, or in the sole discretion of the card brands, may damage the goodwill of the card brands or reflect negatively on the marks.

The card brands consider any of the following activities to be in violation of this rule:

- The sale or offer of sale of a product or service other than in full compliance with the law then applicable to the acquirer, issuer, merchant, cardholder, or the card brands.
- The sale of a product or service, including but not limited to an image, which is patently offensive and lacks serious artistic value (such as, by way of example and not limitation, images of non-consensual sexual behaviour, sexual exploitation of a minor, non-consensual mutilation of a person or body part, and bestiality), or any other material that a card brand deems unacceptable to sell in connection with its mark.

Settlement

You must submit records of a valid transaction no later than three banking days after the transaction date.

Sale or Exchange of Information

You must not sell, purchase, provide, or exchange or in any manner disclose card account number, transaction, or personal information of or about a cardholder to anyone other than your acquirer, to the card brands, or in response to valid government demand. This prohibition applies to card imprints, transaction receipts, carbon copies, mailing lists, tapes, database files, and all other media created or obtained as a result of a transaction.

You must not request or use card account number or personal cardholder information for any purpose that you know or should have known to be fraudulent or in violation of the card brand standards, or for any purpose that the cardholder did not authorize.

Multiple Sales Drafts & Deposit-delayed Delivery Transactions

You must include all goods and services purchased in a single sales transaction (including applicable taxes) in one total amount on a single sales draft.

You are not permitted to process sales transactions if only a part of the amount is included on a sales draft except in the following cases:

- The balance on the amount due is paid by the cardholder at the time of the sales transaction by another payment method(s) in either cash, by cheque or both; or
- The cardholder executes two separate sales drafts if all or a portion of the goods or services will be provided at a later date. In such a case there will be two sales drafts, a deposit may be made by the completion of one sales draft and the payment of the balance is tendered by completion of a second sales draft (with the second sales draft being conditional upon the delivery of the merchandise and/or the performance of services identified). Authorization is required of both sales drafts.
- You shall note on the sales draft the words "deposit" or "balance" as appropriate. The sales draft labelled "balance" shall not be presented until the goods are delivered or the service provided.

Authorization Requirements

- Authorization must be obtained on the date of the transaction.
- If authorization is denied or if the card is not valid or expired, you must not complete the transaction.
- If you process transactions relating to Travel and Entertainment (T&E), ensure the authorization procedures are followed for processing incremental authorization.
- Your compliance with this operating manual and this section does not preclude chargebacks to you under the agreement. For avoidance of doubt, regardless of whether or not a transaction has received an authorization, you always remain responsible for a transaction including but not limited to the following:
  (i) the cardholder is present and does not have his/her card;
  (ii) the cardholder does not sign the sales draft;
  (iii) the signature appears unauthorized or dissimilar to the signature on the card; or
  (iv) the card is expired.

Dynamic Currency Conversion

If you would like to offer dynamic currency conversion or other currency conversion services, you must:

- notify us prior to offering such conversion services to cardholders;
- inform cardholders that the conversion service is optional;
- not impose any additional requirements on cardholders to have Transactions processed in local currency;
- not use any language or procedures that cause the cardholders to choose conversion services by default;
- not misrepresent, either explicitly or implicitly, that the conversion services are provided by the card brands;
- comply with all transaction receipt requirements required by us or the card brands from time to time; and
- comply with any other requirements regarding conversion services that we may notify you of from time to time or as provided for in the card brand rules and regulations.

Returned Merchandise, Credits and Adjustments

For goods and services paid for with a card, you are required to follow a fair policy for refunds, unless otherwise restricted by applicable law. The policies which shall be at least equivalent to such polices as they relate to cardholders who make payment by other methods, unless fully disclosed at the time of the transaction to the cardholder and provided that the sales draft contains a conspicuous notice to that effect prior to completing the transaction.

Failure to disclose your refund or return policy can result in a dispute if your customer returns the merchandise.

Other notes on Refunds:

- Proper disclosure does not include a statement that waives a Cardholder's right to dispute the transaction with its issuer.
- Refunds can only be made on to the card that was used in the original purchase of the goods or services.

- **Recurring Transactions**

  If you agree to accept recurring transactions from a cardholder for the purchase of goods or services which are delivered or performed *on a continued periodic basis* such as monthly, quarterly or annually, the cardholder is required to complete and deliver to you a written request for such goods or services to be charged to the cardholder's account. The written request must at the least specify the transaction amount(s) frequency to cardholder's account, the recurring charges and the duration of time for which such cardholder's permission is granted.

  In the event that a recurring transaction is renewed, the cardholder must complete and deliver to you a subsequent written request for continuation of such goods or services to be charged to the cardholder's account. A recurring transaction may include the payment of recurring charges such as insurance premiums, subscriptions, membership fees, tuition or utility charges.

  Except as stated in this operating manual, a recurring transaction may not include partial payments made to you for goods or services purchased in a single transaction, nor can it be used for occasional payment of goods. The cardholder's written authorization must be retained for the duration of the recurring charges and provided in response to a request from us or the card brands.

  You must not complete an initial or subsequent recurring transaction after receiving a cancellation notice from the cardholder or us or after receiving a response that the card is not to be honoured. You shall type or print legibly on the 'signature line' of the sales draft for recurring transactions, the words 'recurring transaction.'

- **Lost or Stolen Equipment**

  For lost or stolen equipment, contact Moneris immediately at **1-866-319-7450**. If required, a service agent will arrange to have the missing POS equipment replaced. Please note that Moneris merchants are responsible for the security and safe keeping of all rental equipment within their possession. Please refer to your terms and conditions of your merchant agreements for further details.

Payment Card Industry Security Standards

The Payment Card Industry Security Standards Council (PCI SSC) is responsible for the development and ongoing evolution of security standards for cardholder account data protection. The PCI SSC currently manages the following security standards:

- PCI Data Security Standard (DSS)
- PCI PIN Transaction Security (PTS) Standard
- PCI Payment Application Data Security Standard (PA-DSS)

The PCI SSC is also responsible for the training and qualification of security assessors and vendors that validate merchant and service provider compliance against these standards. The PCI SSC is not responsible for enforcing compliance to these standards. Enforcement of compliance is managed independently by the Card Brands.

For more information on the PCI SSC please visit pcisecuritystandards.org.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect cardholder account data.

Below are the twelve principal requirements of PCI DSS that you are required to follow:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

The full text of the PCI DSS and supporting documentation can be found at pcisecuritystandards.org.

Cardholder Data Storage

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether storage of each data element is permitted or prohibited; and if each data element must be protected.

Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/ CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

[1]Sensitive authentication data must not be stored after authorization (even if encrypted).
[2]Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Service Providers

A service provider is defined as an organization that stores, processes, or transmits cardholder data on behalf of merchants or service providers. All service providers are required to comply with PCI DSS. In addition, all service providers are required to validate their compliance to PCI DSS. It is the merchant's responsibility to ensure that any service provider it uses to store, process, or transmit cardholder data is compliant with PCI DSS.

Card Brand Compliance Programs

The card brands have each developed their own compliance program to ensure merchants and service providers are compliant with PCI DSS. Each program has specific validation requirements which must be followed for the card brands to recognize certification to PCI DSS. All merchants and all service providers that store, process, or transmit cardholder data are required to be compliant with PCI DSS.

More information on the card brand compliance programs can be found at:

Visa Canada Account Information Security Program (AIS)
visa.ca/ais

MasterCard Site Data Protection Program (SDP)
mastercard.com/sdp

Discover Information Security & Compliance (DISC) Program
discovernetwork.com/disc

Security Breach

An account data compromise event is defined as cardholder account information that has been accessed without authorization, whether initiated by a disgruntled employee, a malicious competitor, or a misguided hacker. Security breaches can come in the form of a system breach where deliberate electronic attacks on communications or information processing systems occurs or in a form of a physical breach where paper material, payment processing devices, or computer systems that contain cardholder data are physically stolen.

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data:

- Immediately contain and limit the exposure.
- Alert all necessary parties immediately including Moneris.
- Provide Moneris with a detailed description of the events and a list of all card numbers that may have been affected.
- Develop a remediation plan to address the security issues which caused the security breach.

If you have experienced a suspected or confirmed security breach, contact the Moneris Customer Service Centre at 1-866-319-7450 immediately.

If a merchant experiences a security breach which results in the compromise of cardholder data, the merchant may face the following:

- Cost of forensic investigations.
- Non-compliance assessments.
- Cost incurred by card issuers such as card monitoring, card re-issuance, and fraud losses.
- Cost to validate compliance to PCI DSS.
- Termination of card processing services.

Payment Application Data Security Standard (PA-DSS)

Payment Application Data Security Standard (PA-DSS) is a new PCI standard.

PA-DSS (previously known as Visa's Payment Application Best Practice – PABP) is a security standard applicable to payment applications that are developed by software vendors and sold, distributed, or licensed to merchants. The goal of PA-DSS is to help software vendors develop secure payment applications that do not store sensitive data and help support merchant compliance with PCI DSS. All merchants that use third party payment applications are required to ensure that the application meets PA-DSS requirements. To learn more about the PA-DSS compliance mandates and timelines, visit moneris.com/pci.

By using a PA-DSS compliant payment application, you help to decrease the risk of account data compromises, prevent storage of prohibited data and support your responsibility to comply with PCI DSS.

Further information on PA-DSS including a list of validated applications can be found at pcisecuritystandards.org.

E-commerce

Merchant Websites

You must ensure that your website prominently and unequivocally informs the cardholder of the identity of your business at all points of interaction, so that the cardholder readily can distinguish your business from any other party, such as a supplier of products or services to the Merchant.

Your website must contain all of the following information:

- Prominently display your business name.
- Prominently identify your business name as displayed on the website as both your business name and as the name that will appear on the cardholder statement.
- Display your business name as prominently as any other information depicted on the website, other than images of the products or services being offered for sale.
- Card brand marks in full colour to indicate credit/debit card acceptance.
- Complete description of the goods or services offered.
- Company Information and customer service contact information which includes an electronic mail address and telephone number.
- Terms of Service, including export restrictions (if known) or legal restrictions which are clearly displayed at virtual check-out.
- Return/refund policy.
- Customer service contact, including electronic mail address or telephone number.
- Address of the merchant's permanent establishment.
- Transaction currency (e.g., US dollars, Canadian dollars).
- A detailed return and refund policy that informs cardholders of their return or refund options before they purchase a product or service.
- "Click to accept" or alternative affirmative action by the cardholder when completing an online order.
- A printable "receipt" page after the cardholder confirms a purchase.
- Delivery policy.
- Disclosure of the merchant country at the time of presenting payment options to the Cardholder.
- Privacy policy.
- Security capabilities and policy for transmission of payment card details.

Security Requirements/Protecting Your Network

You and your service providers must meet the minimum encryption standards for gathering and transmitting cardholder data such as secure sockets layer (SSL) or 3-D secure. Authorization is required for each e-commerce transaction. You may not refuse to complete an e-commerce transaction solely because the cardholder does not have a digital certificate or other secured protocol.

Verified by Visa (VbV)

Verified by Visa is a global online authentication service that makes online shopping more secure for both Visa merchants and cardholders.

VbV provides your business with added protection against fraudulent transactions and chargebacks for online sales, while providing the cardholders with added confidence while shopping online, which can help to turn browsers into purchasers.

For more information on VbV, visit visa.ca.

MasterCard Secure Code

MasterCard Secure Code is a global e-commerce solution that enables your customers to authenticate themselves to their card issuer through the use of a unique personal password and gives you an indication of a genuine purchaser.

A Secure Code is a private code, known only to the cardholder and his or her financial institution that enhances the cardholder's existing MasterCard account by protecting the cardholders against unauthorized use of their card when shopping online at participating online merchants.

To participate in Secure Code, please call us at 1-866-MONERIS.

For more information on Secure Code, visit mastercard.com.

Card Verification Digits

Card Verification Digits (CVD) is a 3-digit-code which is a security requirement on all Visa, MasterCard, Discover and UnionPay cards. It is found on the back of the cards, printed at the end of the signature panel (see the section *How to Identify Security Features* within this operating manual) or in a white box outside the signature panel. The 3-digit-code is an important security feature that helps merchants validate the authenticity of the cardholder making the purchase.

After submitting a request for authorization for the card information (account number, card expiration date, and 3-digit-code), the merchant receives a response letting the merchant know whether the 3-digit-code is matched or mismatched, allowing you to take appropriate action.

Regardless of the 3-digit-code verification response, if the issuer does not approve the authorization request, you should not complete the transaction.

The 3-digit-code enables merchants operating in an online or phone environment to verify that the cardholder is in physical possession of a genuine card. Visa issuers provide a real-time check of the 3-digit-code to help you verify that the person making the purchase physically has the card in hand.

If you submit the 3-digit-code for authentication and the issuer does not participate in the validation, the merchant will be protected against liability for any potential fraudulent transactions. If a purchaser can only provide the merchant with the 16-digit credit card number and the expiry date, this means that the purchaser likely does not have actual physical possession of the card, signalling a potentially fraudulent transaction.

To learn more about eFraud tools or to speak to a Moneris representative, please call us at 1-866-MONERIS.

For more information, visit visa.ca.

Address Verification Service (AVS)

AVS verifies a cardholder's billing address information in real-time and provides you with a results code separate from the authorization response code, allowing the merchant to make an informed transaction "risk assessment" decision on whether to continue with the transaction.

AVS helps ensure that the person making the purchase with his or her card is the same person who receives the card's monthly statement.

By matching the billing address on file with the card issuer against the billing address provided by the cardholder, merchants and issuers work together to help ensure that lost or stolen cards are not being used in card-not-present environments to purchase goods or services.

Unless the correct billing address is provided to the online, mail or telephone merchant during check-out, the transaction will not be completed which may stop a fraudulent purchase from being made.

IMPORTANT NOTE:

- It is prohibited to store CVD data after authorization has been obtained for the transaction. Please see the *PCI DSS* section within this operating manual.

E-commerce Receipt Requirements

- Merchant name
- Merchant online address
- Transaction amount (or credit), indicated in Transaction Currency
- Transaction date (or credit preparation date)
- Unique transaction identification number
- Purchaser name
- Authorization code
- Transaction type (purchase or credit)
- Description of merchandise/services
- Return/refund policy (if restricted)

Frequently Asked Questions

Q. I have recently upgraded my electronic POS terminal. What should I do with my old equipment?

A. Please return your surplus POS equipment and accessories to Moneris by calling the Moneris Customer Service department at **1-866-319-7450** and we will arrange a courier pick-up for you.

Q. I just received this sales draft/ticket copy/retrieval request, what should I do?

A. Carefully read the information on the sales draft/ticket copy/retrieval request, locate all relevant documentation (receipts, invoices, contracts, etc.) and fax to Moneris at the fax number provided. For more information, please see the section on *Chargebacks* in this operating manual.

Q. I just faxed in the receipt for the transaction in question. How do I know if it was received?

A. Retain your confirmation that is printed by your fax machine, or call Moneris 48 business hours after you send the fax to confirm it has been received.

Q. Can I charge a cardholder a fee for using their Visa, MasterCard, Discover, UnionPay or Interac Direct Payment (Debit) Cards?

A. No. You cannot charge a fee (surcharge) for card use. Regardless of the types of products you sell, it is against your merchant agreement to charge any cardholder a fee for making a purchase with their credit or debit card. Nor can you impose a minimum or maximum transaction value on a purchase where a card is tendered for payment (See the section on *Surcharging* and *Maximum/Minimum* rules within this operating manual).

Q. Our business will be relocating. Whom do I call about our change of address?

A. Please contact our Merchant Customer Service Department if your business changes its ownership, address, phone or fax numbers.

Q. I processed a transaction through my POS terminal and received an authorization code. Why did I then end up receiving a chargeback for this transaction?

A. Notwithstanding the fact that you received an authorization code, you might still receive a chargeback if the cardholder disputes the transaction and/or if proper card acceptance procedures were not followed.

Q. I spoke to the cardholder who later recognized a transaction I processed to his credit card account which resulted in a chargeback. How would I be able to remedy this chargeback?

A. Advise the cardholder to contact his card issuing bank where the dispute originated from and request to withdraw from the dispute or respond to the chargeback by requesting a written statement from the cardholder accepting the charges to his account and fax the document to Moneris.

Q. Am I permitted to ask a cardholder for personal information, such as a telephone number or address, and write this information on the sales draft as an additional measure of security?

A. Never ask a cardholder to write their phone number/address on the sales draft as a matter of routine. You may ask for information only if it is required to complete the transaction such as asking for the delivery address. If you perceive a transaction risk or if the merchant is instructed by Moneris, you may ask for additional identification from the cardholder. (for example I.D.) Once the I.D. is reviewed and the merchant is satisfied they should write "I.D. Checked" in proximity to the cardholder's signature. Under no circumstances should the merchant record the cardholder's I.D. information.

Q. Why is a portion of the cardholder's card number hidden on customer receipts?

A. To reduce the risk of fraudulent card use, only a portion of the cardholder's card number is printed on the cardholder receipt and on some reports. The remainder of the card number is masked, i.e., an '*' is printed for each remaining digit in the card number. Both debit card and credit card numbers (including private label card numbers) are masked. Card masking is also referred to as "card number masking" and "PAN truncation." (See the section on *PAN Truncation* within this operating manual.)

Q. What should I do if a cardholder gives me a letter authorizing him or her to use someone else's card?

A. No one is authorized to use a card, under any circumstances, other than the person whose name and signature appear on it.

Q. How long should I keep copies of my sales/refunds drafts?

A. For credit card transactions 18 months. For debit card transactions 12 months.

Q. If a cardholder pays me by cheque and I use his credit card number as identification, can I process a charge to this credit card for the amount of the cheque if it is returned NSF?

A. No, it is a violation of your merchant agreement to process a charge to a credit card in an attempt to recover uncollectible debt. We suggest contacting the cardholder and arranging for an alternate method of payment.

Q. If a cardholder tells me they don't have their card with them but would like to make a purchase, can I go ahead and complete the sale using the card number and expiry date?

A. No. Do not complete any face-to-face transactions unless the credit card is present and you are able to imprint/swipe or insert/dip the card and obtain the cardholder's signature.

Q. A tourist from the US wishes to purchase a product from my store. Can I quote her the price in US dollars and complete the sales slip for that amount to make it easier for my client?

A. This is permitted if you are a Dynamic Currency merchant; if not, you can only process your transactions in Canadian dollars. The bank which issued your client's credit card will do the currency conversion, and your client will be billed the equivalent amount in US dollars.

Acronyms and Helpful Websites

ABM – Automated Banking Machine
AIS – Account Information Security
AVS – Address Verification Service
CAD – Canadian
CTR – Chargeback to Transaction Ratio
CVD – Card Verification Digits
ECM – Excessive Chargeback Merchant
ECP – Excessive Chargeback Program
GMAP – Global Merchant Audit Program
GMCMP – Global Merchant Chargeback Monitoring Program
IP – Internet Protocol
MCC – Merchant Category Code
MCW – MasterCard Worldwide
MFPP – Merchant Fraud Performance Program
MOTO – Mail Order Telephone Order
NSF – Non-Sufficient Funds
NSR – No Signature Required
PA-DSS – Payment Application Data Security Standard
PAN – Primary Account Number
PCI DSS – Payment Card Industry Data Security Standards
PCI SSC – Payment Card Industry Security Standards Council
PIN – Personal Identification Number
PED – Pin Entry Device
POS – Point of Sale
SDP – Secure Data Program
SSL – Secure Socket Layer
VbV – Verified by Visa

Helpful Links

moneris.com
visa.ca
mastercard.com
discover.com
unionpay.com
interac.ca
pcisecuritystandards.org

Lodging/hotel merchants please visit: **moneris.com** (search hotels)
visa.ca/merchant

Car rental merchants please visit: **visa.ca/merchant**

How to contact us

Our Merchant Customer Service support line is available 24 hours a day, seven days a week to answer any questions you may have regarding your merchant account. Please visit us online at **moneris.com** or call us at **1-866-319-7450**.

To obtain an authorization code using our automated system, call us at **1-866-802-2637**.

If you would like to speak to our Sales department, please call us at **1-866-319-7450**.

How to order stationery/promotional materials

You can order a number of supplies for your business from Moneris. Please visit us online at **shopmoneris.com** or call us at **1-866-319-7450**.

Get an updated manual

Moneris may, from time to time, update this operating manual. You are responsible for ensuring you obtain and are using the most up-to-date copy of the Operating Manual. To obtain an updated copy, please go to **moneris.com/manuals**.

Please note that Visa, MasterCard and Discover have made some rules and regulations publicly available at:
usa.visa.com/merchants/merchant-support,
mastercard.com/ca/merchant/en/getstarted/rules.html, and
discovernetwork.com/merchants/services/.

Moneris SOLUTIONS

MERMAN-E (10/14)