Merchant Operating Manual

Moneris™

BE PAYMENT READY

(05/16)

Moneris™

BE PAYMENT READY

For more information and assistance:

Web: moneris.com

Toll-free: 1-866-319-7450

Record your Moneris® merchant ID here:

____

Contents

About Moneris

Working with Moneris is a decision to stay ahead of the constantly evolving world of payments. As one of North America's largest providers of payment processing solutions, we're on the leading edge of advancements in payment technology. We embrace change so that your business is ready for tomorrow, today.

From flexible in-store terminals, to mobile and E-commerce point-of-sale platforms, innovation is at the forefront of our payment offerings. Not only that, our solutions are backed by reliable and secure technology to ensure a positive experience for your customers.

Keeping on top of change is our job. Keeping customers happy is yours. You've already made the choice to be prepared for what the future may bring.

> Welcome to a new age of being **PAYMENT READY**.

Here’s what you can expect from Moneris:

RELIABLE – Moneris’ **99.9% system reliability*** ensures you can provide a great customer experience.

CONNECTED – Our comprehensive, trusted **E-commerce solutions** help ensure a seamless online shopping experience for your customers, 24/7.

INTEGRATED – Bring it all together with the power of our **integrated business solutions**. Connect POS and reporting, CRM and online sales.

MOBILE – Our **mobile payment solutions** can unleash your potential, from wireless terminals to payment apps that turn any smartphone into a point-of-sale device.

SECURE – Transactions are protected by **industry-leading security standards** that help keep you safe from fraud.

ADVANCED – Payment is just part of the picture. We’re constantly thinking ahead to bring you **innovative business tools** to help you reach your full business potential – today and tomorrow.

*The Moneris service is available if the Moneris host system processing platform is operational. Service availability is measured by Moneris each calendar quarter and is subject to certain exclusions as determined by Moneris.

Processing transactions

Here's what you need to know to begin accepting payments from a customer.

General requirements for 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 can readily 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 ought to know 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.

Proper processing procedures

CHIP TRANSACTIONS

A chip card is a debit or credit card with an embedded microchip that the cardholder inserts into a point-of-sale (POS) terminal card reader. Because chip cards process data securely, it is difficult to copy or tamper with them.

Chip technology helps to:

- Reduce chargebacks
- Reduce fraud
- Simplify store operations

How it works

A transaction using a chip card with a chip-reading POS terminal is simple. Rather than swiping the card and signing a receipt, cardholders insert their chip card into the chip-reading POS terminal and manually

Important things to know about chip transactions

- When presented with a chip card, do not swipe the card first. Simply insert the card and follow the prompts.
- 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.

enter their Personal Identification Number (PIN) using the keypad.

Leave the chip 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 card when prompted. Insert card, chip side up.
4. Follow the prompts.
5. Wait for the "Remove card" message then remove the chip card.

The transaction is complete!

Note: *Some customers may carry a Chip and Signature card that does not require a PIN. Your terminal will recognize the card and prompt you to follow the required payment process.*

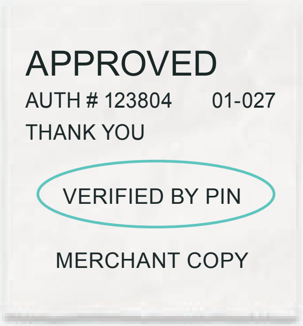
Note: *UnionPay receipts do not display the text "VERIFIED BY PIN". UnionPay transactions require a cardholder signature for all transactions including PIN verified. You may not be protected from chargebacks if you do not obtain the cardholder's signature.*

Important things to know about chip transactions continued...

- 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.

  Note: *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.*

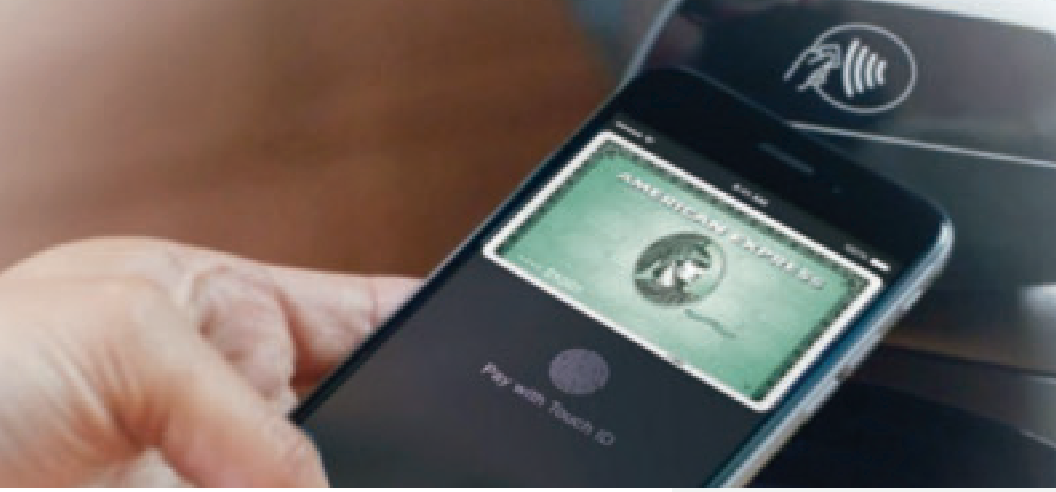
- As a best practice, we recommend that you look at the bottom of the receipt and circle the text "VERIFIED BY PIN".



APPROVED
AUTH # 123804 01-027
THANK YOU

VERIFIED BY PIN

MERCHANT COPY



CONTACTLESS TRANSACTIONS

Contactless transactions are designed to speed up checkout and simplify the payment process for you and your customers.

How it works

Instead of swiping or inserting the card into a terminal, the customer waves or taps the card on the contactless-enabled terminal.

As contactless technology continues to evolve, more cardholder contactless payment devices are becoming increasingly popular (such as mobile phones, smartphones or key fobs). These devices work in the same way as a card, in that the contactless payment is made by waving the cardholder contactless payment device over a contactless-enabled terminal.

Important things to know about contactless transactions

- To accept contactless transactions, you will need a contactless enabled terminal or software system, or a certified contactless reader.
- No signature or PIN is required for transactions under a specified amount. (See *Contactless programs* on page 32.)
- 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.

SWIPED TRANSACTIONS

Here's what to do when a customer presents you with a magnetic stripe card.

Here's what to do

- 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 Moneris Authorization Centre at **1-866-802-2637**.
- If you suspect fraudulent activity, or have any questions regarding transaction authorization, ask for a Code 10 authorization. (See *Code 10 procedures* on page 16.)
- If the Authorization Centre requests that you retain a card, do so only by reasonable and peaceful means. Never put yourself in danger.

MANUAL KEY-ENTERED TRANSACTIONS

There may be times when a customer's chip card or magnetic stripe card does not work. 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

If you use a POS terminal to process transactions, your floor limit is zero and you must obtain an authorization number for each manual key-entered transaction.

***Note:** Manual key-entered transactions are not permitted for UnionPay unless it is to process a hotel or car rental reservation pre-authorization transaction.*

Here’s what to do

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 important components of a card’s security. Manual processing is only appropriate if a card’s chip or 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

Important note about manual key-entered transactions

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.

Note: *Manual key-entered transactions are not permitted for UnionPay unless it is to process a hotel or car rental reservation pre-authorization transaction.*

Key-entered transactions are not recommended for the following reasons:

- 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.

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 **shop.moneris.com** or call Moneris Customer Care 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 reduce fraud for non-chip transactions

Remember, if a card's chip cannot be read, you can help reduce the chance of fraud by following proper processing procedures:

- Look for the hologram, the printed bank identification number, the unique embossed symbol and the signature panel.
- Check the card expiration date.
- If you are satisfied that the card is valid, use the appropriate authorization procedures to request authorization.
- 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.

Important note about manual key-entered transactions continued...

- 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.

Downtime procedures

If you are experiencing system failure, the following procedures must be followed when accepting credit cards:

Note: *These downtime procedures do not apply for UnionPay, as UnionPay cards cannot be accepted when the system is down.*

- Take a manual imprint.
- Phone for voice authorization and record the authorization number on the manual sales draft. Call the Moneris Authorization Centre at **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.

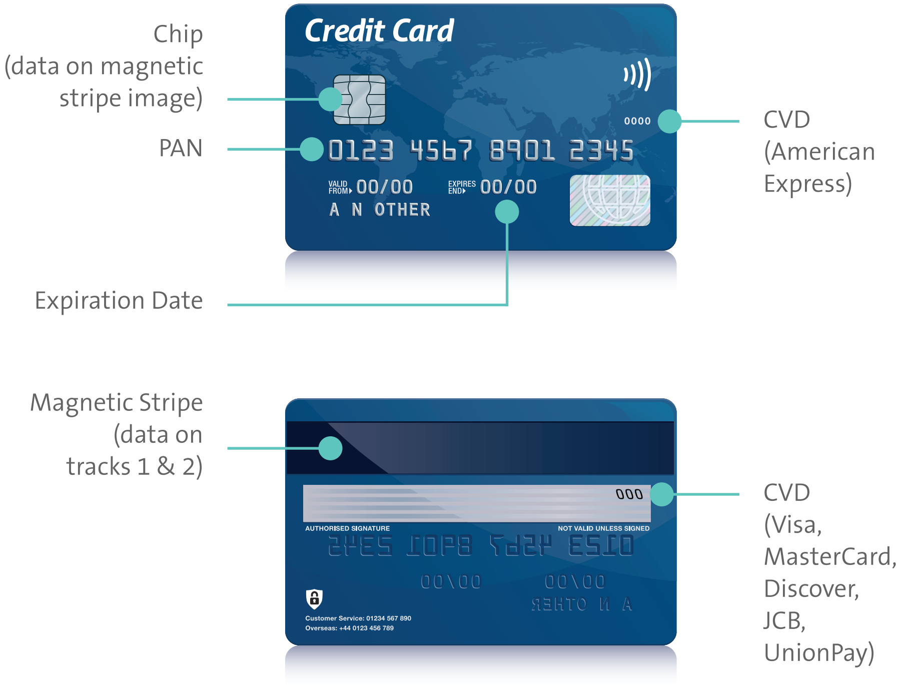
Please ensure that all of the information is clearly visible on the manual sales draft. (See *Manual key-entered transactions* on page 10.)

Protecting your business against fraud

Fraud can be a very real threat to your business. Find out what best practices you can use to help protect your business.

How to identify security features

Types of data on a payment card



Suspicious customer behaviour

Detecting credit card fraud can be 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, or 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 (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.

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* Code 10 procedures *below) which is used when you suspect a card transaction may be fraudulent or suspicious.*

Procedures for lost, stolen, or 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.

Even when proper procedures are followed (e.g., 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.

  Note: *Rewards are at the discretion of the card issuer.*

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

Returning 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:
  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

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.

How it works

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.

There are also portable skimming devices that capture card track data from the magnetic stripe. These devices are often hidden under the counter and have the capacity to run for long periods of time as they can have a larger storage capacity.

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":** When someone looks 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 PIN pad.

- **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 PIN pad. With this type of equipment, the PIN pad 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.

Help cardholders "protect their PIN"

- Cardholders need to be able to enter their PIN without the PIN being seen by others.
- Ensure the POS terminal is installed so that the cardholder can easily shield the PIN pad with their body or that privacy shields are installed if your PIN pad is immovable and/or mounted in a stand.
- Allow the cardholder to hold the PIN pad 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.

Mail order/telephone order (MOTO) 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 orders/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.

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.*

Best practices to help reduce E-commerce fraud

- Authorize all transactions regardless of the dollar amount.
- Implement the applicable fraud prevention tools. (See *Security requirements to protect your network* on page 47.)
- 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 addresses, telephone numbers, signatures, pertinent invoices, and e-mail addresses.
- 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 *Payment Card Industry Data Security Standard (PCI DSS)* on page 41.)

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 the front of their card.
- You can call in for a name and address verification. (See *Address Verification Service (AVS)* on page 49.)

Note: *If you are still suspicious, please do not proceed with the transaction.*

> For more information on protecting your business against fraud, please visit **moneris.com/fraud**.

Chargebacks

A chargeback occurs when a credit or a payment from a transaction, 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, 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, we recommend 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, call Moneris Customer Care at **1-866-319-7450**.

CHARGEBACK REASON CODES

Visit **moneris.com/chargeback** for a list of chargeback reason codes for which your account could be adjusted.

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 time from the transaction date and respond to the request within the timeframe specified in your Merchant Agreement. This varies for each card program: 13 months for Visa®, MasterCard®, and UnionPay, 18 months for Discover® and 24 months for American Express®.

Responding to retrieval requests

If you receive a retrieval request from Moneris, respond to it within the timeframe specified in your Merchant Agreement 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.

Send the documents to Moneris by fax or regular mail:

1. **By fax:**
   - **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.

2. **By mail:**
   Moneris Solutions
   P.O. Box 410 Station “A”
   Toronto, Ontario M5W 1C2

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 kept up-to-date.

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

The document must include the following requirements (and any other document, as requested):

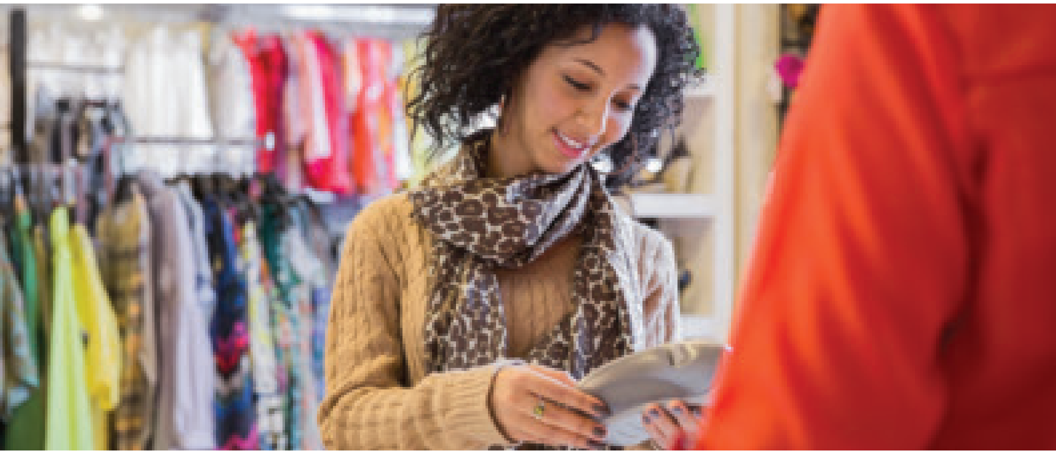
- ✓ Truncated card number
- ✓ Authorization number
- ✓ Cardholder name
- ✓ Cardholder signature (if applicable)
- ✓ Merchant name
- ✓ Merchant location
- ✓ Transaction date
- ✓ Transaction amount

Please also include the original retrieval request with the document.

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.*

Useful tips for 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. For online transactions, ensure the business name on the receipt 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.



MERCHANT DIRECT

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

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

Important standards

- 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.

  Note: *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 Visa, Discover, and American Express, a 20% variance is allowed to restaurants for gratuity purposes only. Therefore the actual (or final) amount must not exceed 20% from the authorization amount.
- For UnionPay, a 15% variance is allowed to restaurants for gratuity purposes only. Therefore the actual (or final) amount must not exceed 15% 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, 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 (3) 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 Order/Phone Order or E-commerce transaction can be obtained up to seven (7) calendar days of the transaction date. For such a transaction, the transaction date is the date the merchandise is shipped.

Card brand programs

The card brands keep an eye on fraud and chargeback rates to the benefit of all merchants accepting their cards.

Note: *Visa, MasterCard, Discover, and American Express have made some rules and regulations publicly available at:*

- **visa.ca/merchant**
- **mastercard.com/ca/merchant**
- **discovernetwork.com/merchants/services**
- **americanexpress.ca/optblueguide**

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 will 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. Merchants often 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.

As a merchant, you may belong to some of the following card brand programs:

Note: *Each Visa, MasterCard, Discover, UnionPay, and American Express 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.*

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 substandard 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.

American Express program

The American Express program monitors for disproportionate chargeback and fraud performance.

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" (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.

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

Other programs

Discover No Signature Required (NSR) program

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).
- The card is swiped and transaction is authorized.
- The card Sale took place in a Card Present environment.
- Must be magnetic stripe transactions only; not applicable to chip transactions.

American Express No Signature/No PIN program

The American Express No Signature/No PIN program allows merchants not to request a signature or a PIN from cardholders on the transaction receipt. The established threshold to qualify under the American Express No Signature/No PIN program is $50.00 or less CAD (including tips and taxes). A receipt does not need to be provided to the cardholder as part of the American Express No Signature/No PIN program unless the cardholder specifically requests a receipt.

To qualify for the American Express No Signature/No PIN program, a transaction must have the following characteristics:

- The transaction value must be less than or equal to $50.00 CAD (including tips and taxes).
- Transaction must be authorized.
- Transaction took place in a Card Present environment.

If the transaction does not meet all three of the qualifying criteria, the American Express No Signature/No PIN program does not apply.

Contactless programs

No signature or PIN is required for contactless transactions under a specified amount (see below for program details).

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.

Contactless Program	The Contactless Program applies to transactions less than or equal to:	Proper procedures for transactions above the set dollar limit:
Visa payWave	$100.00 CAD (including tips and taxes)	Obtain the Cardholder's signature for transactions over $100.00 CAD.
MasterCard TAP & GO™	$100.00 CAD (including tips and taxes)	Transactions over $100.00 CAD must be processed using another payment method. Have the Cardholder insert or swipe their 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.
Interac Flash	$100.00 CAD (including tips and taxes)	Transactions over $100.00 CAD must be processed using another payment method. Have the Cardholder insert their card.
Discover ZIP	$50.00 CAD (including tips and taxes)	Obtain the Cardholder's signature for transactions over $50.00 CAD.
American Express	$100.00 CAD (including tips and taxes)	Obtain the Cardholder's signature for transactions over $100.00 CAD.

> For more information on contactless programs, please visit **moneris.com/quickservice**.

Card acceptance standards

Card acceptance comes with a set of standards merchants are asked to follow. Here they are:

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 (4) 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.

Note: Interac *advises that an abbreviated version of the PAN may be used if it accurately identifies 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, UnionPay, and American Express 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.

Surcharging and convenience fees

You must not add any surcharges or 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,
- 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,
- Arises from the dishonour of a cardholder's personal cheque,
- 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 (3) 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 and 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 is a critical step in the card acceptance process.

- 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:
  - the cardholder is present and does not have his/her card;
  - the cardholder does not sign the sales draft;
  - the signature appears unauthorized or dissimilar to the signature on the card; OR
  - the card is expired.

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 shall be at least equivalent to such policies 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.
- 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 onto the card that was used in the original purchase of the goods or services.

Multi-Currency conversion

Moneris provides two multi-currency services: Dynamic Currency Conversion (DCC) which provides merchants the ability to process card present (face-to-face) transactions in a cardholder's home currency, and Multi-Currency Pricing which provides merchants the ability to process transactions in different currencies in a card not present (E-commerce) environment. If you provide or ask us to provide you with dynamic currency conversion or other currency conversion services, you must:

- Inform cardholders that the conversion service is optional;
- Ensure that the Cardholder is the only party to opt-in or opt-out of a Multi-Currency Transaction;
- Not impose any additional requirements on cardholders to have transactions processed in a cardholder's home 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.

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 the 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 a subsequent written request to you 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 Moneris, or after receiving a response that the card is not to be honoured.

On the 'signature line' of the sales draft, please type or legibly print the words 'recurring transaction' for recurring transactions.

Lost or stolen equipment

For lost or stolen equipment, please contact Moneris Customer Care immediately at **1-866-319-7450**. If required, a service agent will arrange to have the missing POS equipment replaced.

Note: *Moneris merchants are responsible for the security and safekeeping of all rental equipment within their possession. Please refer to your terms and conditions of your Merchant Agreement for further details.*

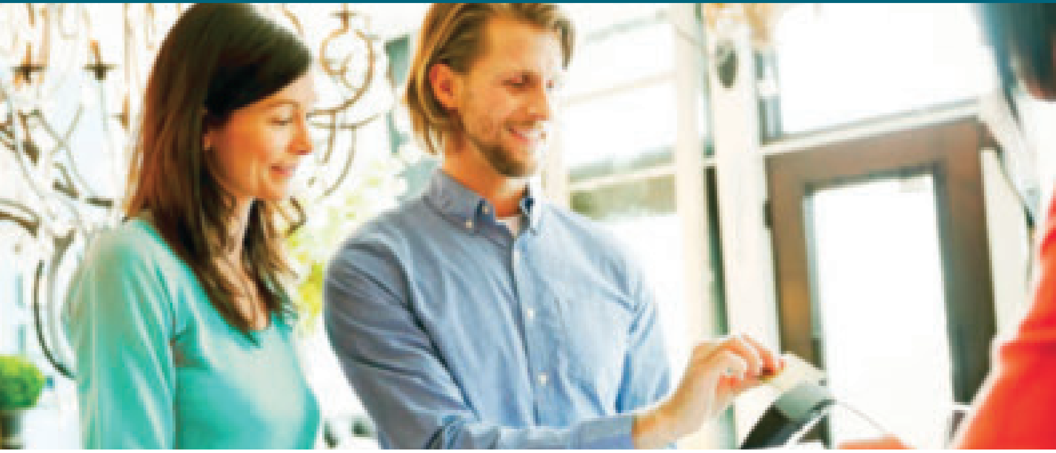
Payment Card Industry Security Standards

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 (PCI DSS)
- PCI PIN Transaction Security Standard (PTS)
- 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 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)	✓	✓
		Cardholder Name	✓	x
		Service Code	✓	x
		Expiration Date	✓	x
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	x	Cannot store per Requirement 3.2
		CAV2/CVC2/ CVV2/CID	x	Cannot store per Requirement 3.2
		PIN/PIN Block	x	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.

Learn more about card brand compliance programs here:

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 breaches

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, please contact Moneris Customer Care immediately at **1-866-319-7450**.

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; and
- Termination of card processing services.

Payment Application Data Security Standard (PA-DSS)

PA-DSS 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.

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.

> To learn more about the PA-DSS compliance mandates and timelines, visit **moneris.com/pci**.

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

E-commerce

Here are some things you need to know if you are running an online store.

Setting up your merchant website

You must ensure that your website clearly 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 and debit card acceptance
- ✓ Complete description of the goods or services offered
- ✓ Company information and customer service contact information which includes:
    - E-mail address
    - Telephone number
    - Address of the merchant’s permanent establishment
- ✓ Terms of Service, including export restrictions (if known) or legal restrictions which are clearly displayed at virtual checkout
- ✓ Return/refund policy, detailing the return or refund options before they purchase a product or service
- ✓ Transaction currency (e.g., US dollars, Canadian dollars)
- ✓ “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

Your *E-commerce receipt* must contain all of the following information:

- ✓ 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 and/or services
- ✓ Return and refund policy (if restricted)

Security requirements to protect your network

You and your service providers must meet the minimum encryption standards for gathering and transmitting cardholder data. 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.

> To participate in VbV, please call us at **1-866-666-3747**.
For more information on VbV, visit **visa.ca**.

MasterCard SecureCode®

MasterCard SecureCode 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 SecureCode is a private code, known only to the cardholder and his or her financial institution, which 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 SecureCode, please call us at **1-866-666-3747**.
For more information on MasterCard SecureCode, visit **mastercard.ca**.

Card Verification Digits (CVD)

Card Verification Digits (CVD) are a security requirement on credit cards. It is a 3-digit-code found on the back of the cards, printed at the end of the signature panel or in a white box outside the signature panel for Visa, MasterCard, Discover, and UnionPay and a 4-digit-code on the front of cards for American Express. (See *How to identify security features* on page 14.)

After submitting a request for authorization for the card information (account number, card expiration date, and CVD), the merchant receives a response letting the merchant know whether the CVD is matched or mismatched, allowing you to take appropriate action. Regardless of the CVD verification response, you should not complete the transaction if the issuer does not approve the authorization request.

The CVD 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 CVD to help you verify that the person making the purchase physically has the card in hand.

If you submit the CVD 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 cardholder can only provide the merchant with the 16-digit credit card number and the expiry date, this means that the cardholder likely does not have actual physical possession of the card, signaling a potentially fraudulent transaction.

> To learn more about e-fraud tools, visit **moneris.com/fraudtools** or call us at **1-866-666-3747**.

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.

Note: *It is prohibited to store CVD data after authorization has been obtained for the transaction. (See* Payment Card Industry Data Security Standard (PCI DSS) *on page 41.)*

Frequently asked questions

We have put together a list of the most frequently asked questions and answers from merchants.

Processing transactions

Q. **Can I charge a cardholder a fee for using their Visa, MasterCard, American Express, Discover, UnionPay, or *Interac* 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 page 34.)

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. **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 due to Non-Sufficient Funds (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. **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 (see *Multi-Currency conversion* on page 38). If you are not a Dynamic currency merchant, 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.

Protecting your business against fraud

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. 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 asterisk (*) 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 *Primary Account Number (PAN) truncation (card masking)* on page 33.)

Chargebacks

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. (See *Chargebacks* on page 22.)

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

A. For credit card transactions, please keep copies of your sales and refunds drafts for 13-24 months depending on the card program. (See *Retrieval Requests* on page 23.) For debit card transactions, please keep copies of your sales and refunds drafts for 12 months.

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.

Other

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 Moneris Customer Care at **1-866-319-7450** and we will arrange a courier pick-up for you.

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

A. Please contact Moneris Customer Care at **1-866-319-7450** if your business changes its ownership, address, phone or fax numbers.

Other resources

Need help?

Please contact Moneris Customer Care toll-free at **1-866-319-7450** (available 24/7).

- To obtain an authorization code using our automated system, please call us at **1-866-802-2637**.
- If you would like to speak to our Sales department, please call us at **1-866-666-3747**.

Get an updated manual

Moneris may periodically update this operating manual at **moneris.com/manuals**. You are responsible for ensuring you obtain and use the most up-to-date copy.

Take your business further

MERCHANT DIRECT

24/7 access to daily card transactions, monthly statements, reporting and more.

Visit **moneris.com/merchantdirect**

SHOP AND STOCK

Conveniently shop for all of your payment acceptance supplies, including paper rolls, decals, signs and more.

Visit **shop.moneris.com** or call Moneris Customer Care at **1-866-319-7450**

THE INSIDE ADVANTAGE

Moneris is committed to keeping you informed of market insights, education, and industry trends through our Moneris Insights Hub.

Visit **moneris.com/insights**

Helpful links

- **moneris.com**
- **visa.ca**
- **mastercard.ca**
- **discover.com**
- **unionpay.com**
- **interac.ca**
- **americanexpress.ca**

Note: *Visa, MasterCard, Discover, and American Express have made some rules and regulations publicly available at:*

visa.ca/merchant

mastercard.com/ca/merchant

discovernetwork.com/merchants/services

americanexpress.ca/optblueguide

Notes

Moneris™

BE PAYMENT READY

moneris.com

MERMAN-E (05/16)