Your Payments Acceptance Guide

May 2020

Welcome

From Start to Finish

A Guide to Accepting Payments

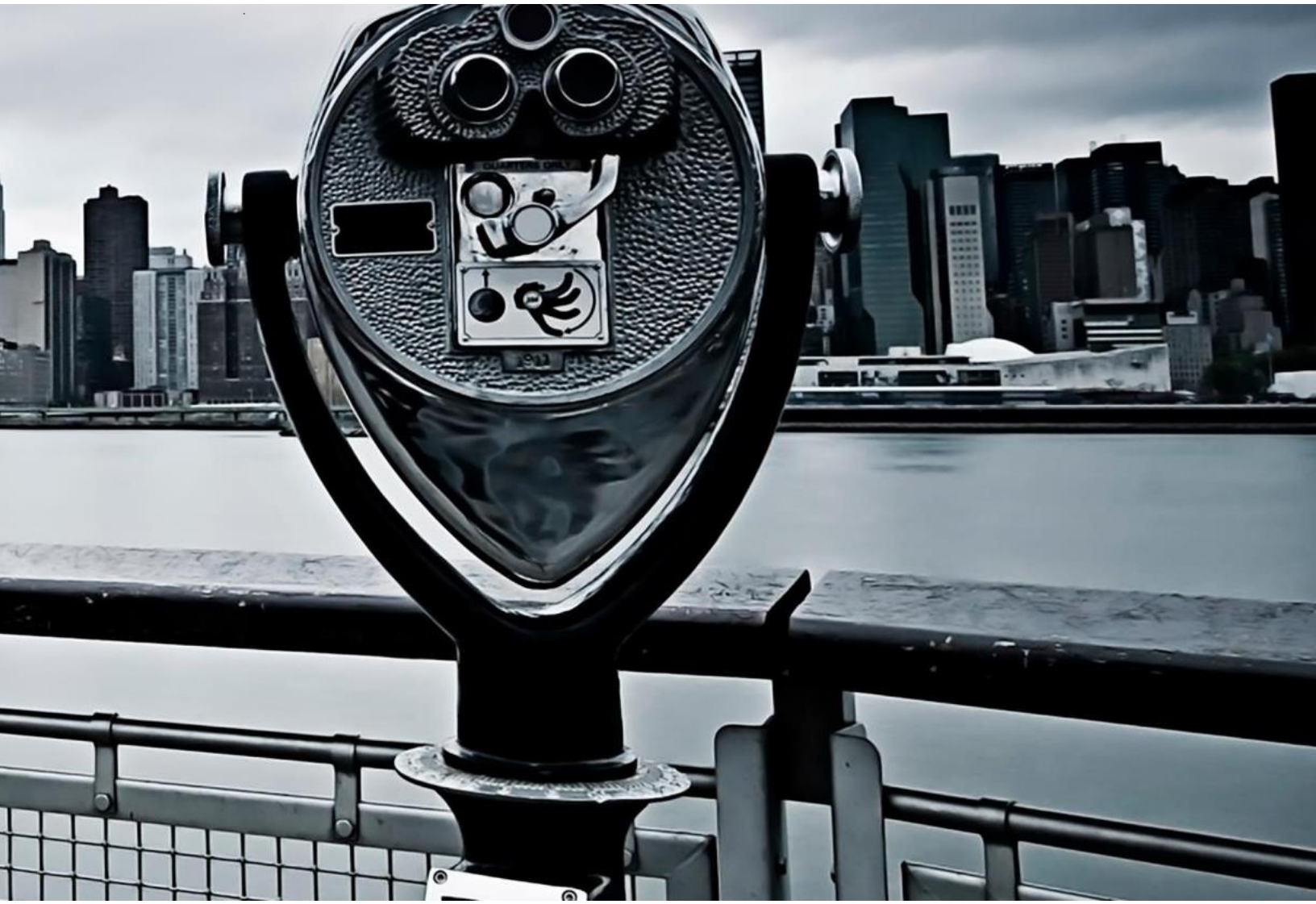
Payment acceptance solutions are an essential part of your business. As your partner, we want to make accepting payments as simple as possible for you. That's why we created Your Payments Acceptance Guide. It's your quick reference to the guidelines for processing transactions. You will also find recommendations and tips to help you prevent fraud, reduce chargebacks, properly handle payments, refunds, exchanges and most other situations you will encounter in your day-to day-business.

If you have questions about processing payments or other aspects of your merchant arrangement, please contact the Fiserv Customer Support Hotline in your country (Lines are open from 9:00 a.m. till 11:00 p.m. after which Interactive Voice System is available for Authorisation only):

Hong Kong: +852 3071 5008

Malaysia: +60 3 6207 4888

Singapore: +65 6622 1888



Your Payments Acceptance Guide Contents

Part I

I. General Guidelines

Fiserv provides processing services to facilitate the transfer of your Sales Receipts back to the thousands of card-issuing institutions. This part of **Your Payments Acceptance Guide** describes the procedures for submitting Card Scheme transactions for payment, obtaining Authorisations, responding to Chargebacks, media retrieval requests and other aspects of the operations of our services. This guide is designed to provide you with the principles for a sound Card program and help you decrease your Chargeback liability and to train your employees.

The content contained in this document focuses primarily on acceptance practices associated with Mastercard, Visa, JCB, Diners and UnionPay. Fiserv provides Authorisation, processing or settlement of Transactions involving other Card Scheme brands, you should also consult those independent Card Schemes to acquaint yourself to their rules and regulations.

The requirements set out in this acceptance guide will apply unless prohibited by law. You are responsible for following any additional or conflicting requirements imposed by your country.

The first step of a Transaction actually begins before a customer even decides to make a purchase. This part of **Your Payments Acceptance Guide** reviews steps you will need to take to ensure customers are informed of their payment options and understand the terms of sale.

1. Use of Card Scheme Brands

Dos

- Prominently display relevant trademarks of the Card Schemes at each of your locations, in catalogues, on websites and on other promotional material
- Only use the official trademarks of Fiserv and of the Card Schemes as officially instructed to do so

Don’ts

- Don’t indicate that Fiserv or any Card Scheme endorses your goods or services
- Don’t use the trademarks of any Card Scheme after: Your right to accept the Cards of that Card Scheme has ended; or that Card Scheme has notified you to stop using their trademarks
- Don’t use the trademarks of Fiserv or of the Card Schemes in any way that injures or diminishes the goodwill associated with the trademarks
- Don’t use the trademarks of Fiserv or the Card Schemes in any manner, including in any advertisements, displays or press releases, without our prior written consent

2. Validating Card Brands

Fiserv acquires for the following Card Schemes: Visa, Mastercard, UnionPay, JCB and Diners.

If you have selected to accept these brands you must honour to accept all Cards presented under these brands with the following logos.

Additionally, Fiserv may make provision for the acceptance and on-forwarding of Transactions for American Express. You will need to engage the American Express separately for contractual arrangements which will include processing, funding and providing you with a statement.

3. Point-of-Sale (POS) Reminders

Dos

You must clearly and conspicuously:

- Disclose all material terms of sale, refund and other policy (if applicable) to be disclosed prior to obtaining an Authorisation
- At all points of interaction inform Cardholders which entity is making the sales offer, so that the Cardholders can clearly distinguish you from any other party involved in the interaction
- Disclose any surcharge/discount/incentive associated with the transaction

4. Transactions Where the Cardholder Is Not Present – Card-Not-Present (CNP) Transactions

This section applies to any Transaction where the Cardholder is not present, such as mail order/telephone order (MO/TO), Internet/e-commerce.

You may only conduct e-commerce Transactions if you have notified us in advance and received approval to do so.

If you accept orders through the Internet, your website must include the following information in a prominent manner:

- A complete description of the goods or services offered
- Details of your (i) delivery policy; (ii) consumer data privacy policy; (iii) cancellation policy; and (iv) returns policy
- The Transaction currency
- The customer service contact, including email address and telephone number
- Your address
- The Transaction security used on your website
- Any applicable export or legal restrictions
- Your identity at all points of interaction with the Cardholder

Dos

- Obtain the Card account number, name as it appears on the Card, expiration date of the Card and the Cardholder's statement address
- Notify the Cardholder of delivery timeframes and special handling or cancellation policies
- Ship goods within seven (7) days from the date on which Authorisation was obtained. If delays are incurred (for example, out of stock) after the order has been taken, notify the Cardholder and obtain fresh Authorisation of the Transaction.
- For e-commerce, add a "tick box" or acceptance confirmation so the Cardholder acknowledges the terms and conditions of the sale they are entering into prior to completing the checkout

Don'ts

- Don't accept Card numbers by electronic mail (email)
- Don't exceed the percentage of your total payment Card volume for Card-not-present sales, as set out in your application
- Don't submit a Transaction for processing until after the goods have been shipped or the service has been provided to the Cardholder – the only exception to this is where the goods have been manufactured to the Cardholder's specifications and the Cardholder has been advised of the billing details
- Don't require a Cardholder to complete any documentation that displays the Cardholder's account number in clear view when mailed or send any mailing to a Cardholder that displays personal information in clear view

5. Transaction Guidelines

Dos

- Only present for payment valid charges that arise from a Transaction with a bona fide Cardholder
- Only present for payment valid charges that arise from a bona fide purchase of goods or services in the ordinary course of your business
- Ensure Transaction amounts reflect the inclusion of Goods and Services Tax (GST), if applicable
- Disclose any surcharge to be applied

Don'ts

- Don't set a minimum Transaction amount for any Card Scheme. Don't establish any special conditions for accepting a Card other than allowable by law (for example, surcharge)
- Don't make any cash disbursements or cash advances to a Cardholder as part of a Transaction with the exception of the cheque/savings Transactions performed with Cards
- Don't require a Cardholder to supply any personal information for a Transaction (for example, phone number, address, driver's licence number and so on) unless required delivery purposes
- Don't submit any Transaction representing the refinance or transfer of an existing Cardholder obligation which is deemed uncollectible, for example, a Transaction that has been previously charged back, or to cover a dishonoured cheque
- Don't submit Transactions on the personal Card of an owner, partner, officer or employee of your business establishment or of a guarantor who signed your application form, unless such Transaction arises from a bona fide purchase of goods or services in the ordinary course of your business

6. Security

You are responsible for maintaining the security of your POS devices, particularly if the device is the asset of Fiserv and for instituting appropriate controls to prevent employees or others from submitting credits (For example, refunds) that do not reflect bona fide returns or reimbursements of earlier Transactions.

Please comply with the data security requirements shown below:

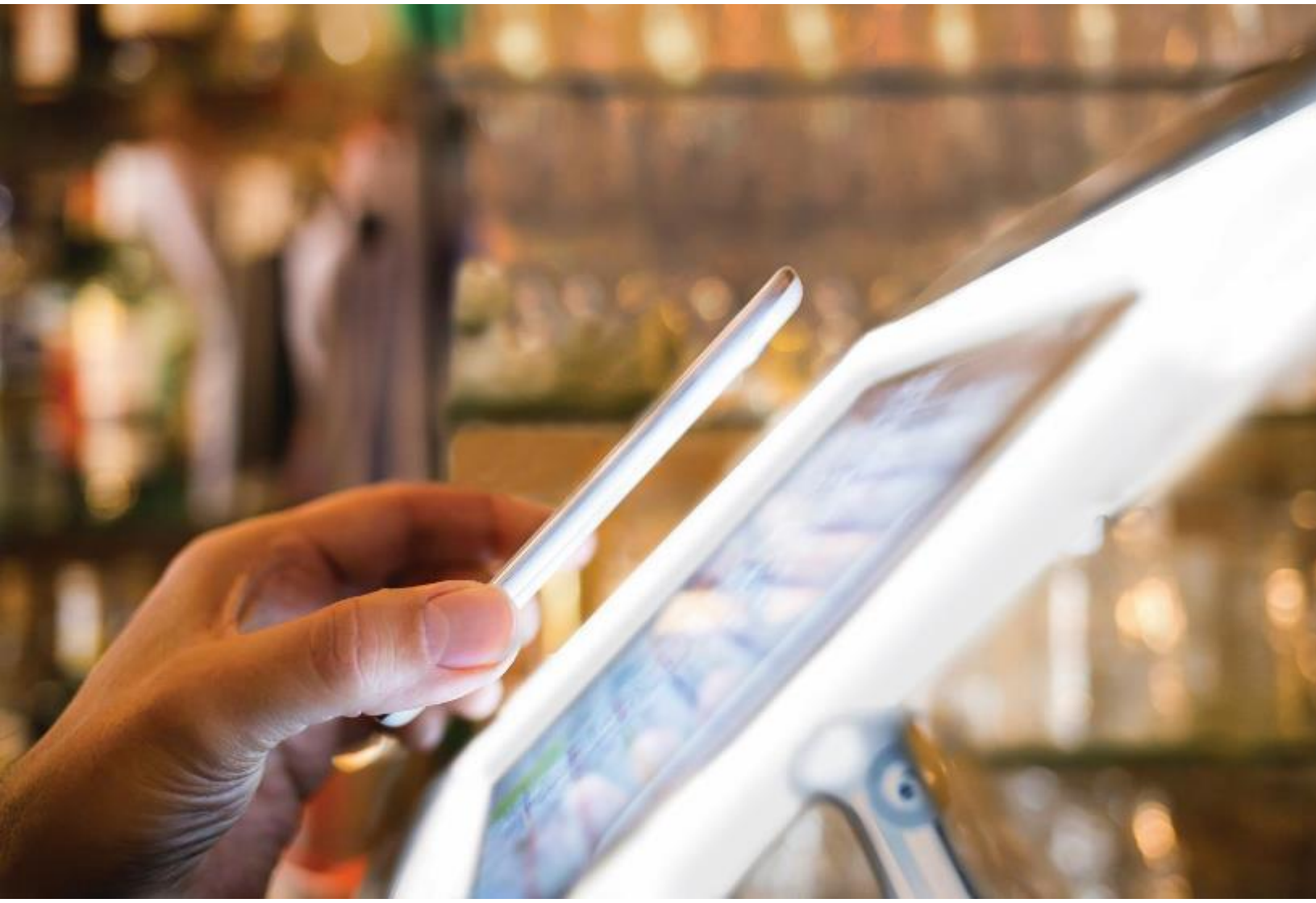
Dos

- Install and maintain a secure firewall configuration to protect data
- Protect stored data, and encrypt transmission of data sent across open/public networks, using methods indicated in the Payment Card Industry Data Security Standard (PCI DSS) which is available at: pcisecuritystandards.org
- Use and regularly update anti-virus software and keep security patches up-to-date
- Restrict access to data by business “need to know” basis. Assign a unique ID to each person with computer access to data and track access to data by unique ID
- Regularly test security systems and processes
- Maintain a policy that addresses information security for employees and contractors
- Restrict physical access to Cardholder information
- Destroy or purge all media containing obsolete Transaction data with Cardholder information
- Keep all systems and media containing Card account, Cardholder or Transaction information (whether physical or electronic) in a secure manner so as to prevent access by, or disclosure to any unauthorised party
- Use only those services and devices that have been certified as PCI-DSS compliant by the Card Schemes and other regulatory bodies

Don’ts

- Don’t use vendor-supplied defaults for system passwords and other security parameters
- Don’t store or retain Card verification codes (three digit codes printed in the signature panel of most Cards) after final Transaction Authorisation
- Don’t store or retain Chip data, magnetic stripe data or PIN data – only Cardholder account number, Cardholder name and Card expiration date may be retained subsequent to Transaction Authorisation

For Internet Transactions, copies of the Transaction records may be delivered to Cardholders in either electronic or paper format.



Part II

II. Information and Guidelines for Specific Transaction Types

This part of **Your Payments Acceptance Guide** reviews essential elements of a Transaction, including Authorisations, issuing refunds and exchanges, and handling special Transactions like recurring payments. You'll also find information about Chargebacks and processes to put in place to help avoid Chargebacks. Feel free to contact the Fiserv Customer Support Hotline with any questions that arise as you review this information.

7. Authorisations

General

- You must obtain an Authorisation approval code for all Transactions
- An Authorisation approval code only indicates the availability of funds on an account at the time the Authorisation is requested. It does not indicate that the person presenting the Card is the rightful Cardholder, nor is it a promise or guarantee that you will not be subject to a Chargeback or adjustment.
- You must not attempt to obtain multiple Authorisations for a single Transaction. If a sale is declined, do not take alternative measures with the same Card to obtain an approval of the sale from other sources. Request another form of payment instead.
- If you fail to obtain an Authorisation approval code or if you submit a Card Transaction after receiving a decline (even if a subsequent Authorisation attempt results in an Authorisation approval code), your Transaction may result in a Chargeback
- You may be charged for a request for an Authorisation approval code (where applicable), whether or not the Transaction is approved
- For Card present Transactions, you must use your Fiserv provided terminal to obtain an Authorisation approval code
- Follow the prompts on the Fiserv provided terminal screen, do not deviate from the prompts or ignore the Authorisation response received

Card-Not-Present Transactions

You will need to obtain the three-digit Card verification code (reflected on the back of the Card) and include this code with each Card-not-present Authorisation request unless the Transaction is a recurring Transaction.

For recurring Transactions, submit the Card verification code only with the first Authorisation request and not with subsequent Authorisation requests.

You should not store Card verification codes.

Transaction Processing

The following general requirements apply to all Debit Card Transactions:

- All debit Transactions must be authorised and processed electronically
- You may not complete a Debit Card Transaction that has not been authorised. If you cannot obtain an Authorisation at the time of sale, you should request another form of payment from the customer or process the Transaction as a Store and Forward or Resubmission, in which case you assume the risk that the Transaction fails to authorise or otherwise decline.
- For a declined Transaction, the Cardholder should be instructed to contact the Issuer to find out why
- Debit Card Transactions must be completed either with a Personal Identification Number (PIN) or without PIN by getting the Cardholder to sign on chargeslip or through means of a contactless "tap and go" method
- Where a PIN must be entered, it must be entered into the PIN pad only by the Cardholder. You cannot accept the PIN from the Cardholder verbally or in written form.
- You must provision for and offer to issue a receipt to the Cardholder upon successful completion of a Transaction
- The Cardholder account number will be masked so that only the part of the account number (For example, first six and last three digits) will appear. The masked digits will appear as a non-numeric character such as an asterisk. This is referred to as PAN truncation.
- You may not manually enter the account number. The account number must be read electronically from either the Chip or the magnetic stripe which is used in the event of "technical fallback" when the terminal cannot interact with the Chip.
- If the magnetic stripe is also unreadable, you must request another form of payment from the Cardholder
- Any applicable tax (for example, GST) must be included in the total Transaction amount for which Authorisation is requested. Tax may not be collected separately in cash.
- You are responsible to secure your terminals, terminal passwords and change to its default passwords and to institute appropriate controls to prevent employees or others from submitting Refunds and voids that do not reflect bona fide returns or reimbursements of prior Transactions
- You must not store any PIN and you must securely store any account information to prevent unauthorised access, use or disclosure

8. Special Types of Transactions

Payment by Instalments

If a Cardholder makes a deposit toward the full amount of the sale price and pays the balance on delivery, please follow the procedures set out in this section.

Dos

- Execute two separate Transactions and obtain an Authorisation for each on each Transaction date
- Submit and seek Authorisation of each delayed delivery Transaction under the same merchant identification number and treat deposits on the Card no differently than you treat deposits on all other payment products
- Obtain proof of delivery upon delivery of the services/merchandise purchased

Don'ts

- Don't submit a final Transaction to us relating to the "balance" until the goods have been completely delivered or the services fully provided

Recurring Transactions

If you process recurring Transactions and charge a Cardholder's account periodically for goods or services (For example, yearly subscriptions, annual membership fees and so on) please follow the procedures set out in this section.

Dos

- Obtain written Cardholder approval for goods or services to be charged on a recurring basis to the Cardholder's account. Approval must at least specify:
  - The Cardholder's name, address, account number and expiration date
  - The Transaction amounts
  - The timing or frequency of recurring charges
  - The duration of time for which the Cardholder's approval is granted
- Obtain an Authorisation for each Transaction
- Include the recurring payment indicator in each Authorisation request, and as applicable, each batch submission entry

Don'ts

- Don't include partial payments for goods or services purchased in a single Transaction
- Don't impose a finance charge in connection with the recurring Transaction or preauthorised order
- Don't complete a recurring Transaction after receiving a cancellation notice from the Cardholder or Card issuing bank or after a request for Authorisation has been denied

It is highly recommended that you obtain the three-digit Card verification code on the back of the Card and include the number with the first Authorisation request. This is not required for subsequent Authorisation requests.

You should not store Card verification codes.

A positive Authorisation response for one recurring Transaction is not a guarantee that any future recurring Transaction Authorisation request will be approved or paid.

If the recurring Transaction is renewed, you must obtain from the Cardholder a new written request for the continuation of such goods or services to be charged to the Cardholder's account.

If you or Fiserv have terminated your right to accept Cards, you must not submit Authorisation requests or Transactions for recurring Transactions due after the date of such termination.

Stored Payment Credentials

If you store information (including, but not limited to, an account number or payment token) to process future purchases on behalf of the Cardholder, follow the procedures set out in this section.

Dos

- Do include the appropriate data values when a payment credential is being stored for the first time
- Do include the appropriate data values when a payment credential is being used to initiate a stored credential Transaction
- Do include the appropriate data values when a payment credential is being used to identify an unscheduled credentials on file Transaction
- Do submit a valid Authorisation if an amount is due at the time the payment credential is being stored
- Do submit an Authorisation verification if no payment is due at the time the payment credential is being stored

Don'ts

- Don't store a payment credential if either the first payment Transaction or account verification is declined

9. Refunds

Dos

- For e-commerce, do add a "tick box" or acceptance confirmation so the Cardholder acknowledges the terms and conditions of the sale they are entering into prior to complete the checkout
- Provide clear instructions to your customers regarding returns, including the following
  - Customer service telephone number
  - Reference number for the return
  - Expected processing time for the credit
  - Return address, preferably on a pre-formatted shipping label (if applicable)
- Do document your cancellation policy as applicable to local laws
- Do provide full Refunds for the exact dollar amount of the original Transaction including goods and services tax and in no circumstances provide a Refund amount for more than the original sale amount

Don’ts

- Don’t provide a Refund amount for more than the original sale amount
- Don’t credit an account that differs from the account used for the original Transaction
- Don’t give cash, cheque or other consideration for Card sales
- Don’t intentionally submit a sale and an offsetting credit at a later date solely for the purpose of debiting and crediting your own or a customer’s account
- Don’t process a Refund after a Chargeback has been received

Your website must communicate your refund policy to your customers with the prudent practice of seeking your customers to select a “click-to-accept” or another affirmative button to acknowledge the policy.

Display the terms and conditions of the purchase on the same screen view as the checkout screen that presents the total purchase amount, or within the sequence of website pages the Cardholder accesses during the checkout process.

10. Chargebacks, Retrievals and Other Debits

Chargebacks

Both the Cardholder and the Card issuing bank have the right to question or dispute a Transaction. If such questions or disputes are not resolved, a Chargeback may occur. You are responsible for all Chargebacks, our Chargeback fees and related costs arising from your Transactions. As a result, we will debit your settlement account for the amount of each Chargeback.

Due to the short time frames and the supporting documentation necessary to successfully (and permanently) reverse a Chargeback in your favour, we strongly recommend that:

- You adhere to the guidelines and procedures outlined in this guide
- Investigate if you receive a Chargeback, submit the appropriate documentation within the required time frame if you dispute the Chargeback
- Whenever possible, contact the Cardholder directly to resolve the dispute
- If you have any questions, call the Fiserv Customer Support Hotline, contact your account manager or write to chargebacks@firstdatams.com

You must not process a credit Transaction (also known as a Refund) once a Chargeback is received, even with Cardholder Authorisation, as the credits may not be recoverable and you may be financially responsible for the credit as well as the Chargeback. Instead, the Card issuing bank will credit the Cardholder’s account.

Chargeback Process

If the Card issuing bank submits a Chargeback, we will send you a Chargeback notification, which may also include a request for Transaction documentation. Due to the short time requirements imposed by the Card Schemes, it is important that you respond to a Chargeback notification request promptly and within the time frame set out in the notification.

Upon receipt of a Transaction documentation request, you must immediately retrieve the requested Transaction receipt/sales draft(s) using the following guidelines:

- A legible copy
- If applicable, make copies of a hotel folio, car rental agreement, mail/phone/Internet order form or other form of receipt
- Submit supporting documentation in accordance with the instructions provided

If the information you provide is both timely and, in our sole discretion, sufficient to warrant a re-presentment of the Transaction or reversal of the Chargeback we will do so on your behalf. A re-presentment or reversal is ultimately contingent upon the Card issuing bank and/or Cardholder accepting the Transaction under applicable Card Schemes guidelines. Re-presentment or reversal is not a guarantee that the Chargeback has been resolved in your favour.

If we do not receive a clear, legible and complete copy of the Transaction documentation within the timeframe specified on the request, you may be subject to a Chargeback for "non-receipt" for which there is no recourse.

If you do not dispute the Chargeback within the applicable time limits as set by the Card Schemes rules and regulations, you will forfeit your reversal rights.

If we reverse the Chargeback and re-present the Transaction to the Card issuing bank, the Card issuing bank, at its sole discretion, may elect to submit the matter for arbitration before the applicable Card Scheme. The Card Scheme may charge a filing fee and a review fee. Whether or not a decision is made in your favour, you will be responsible for all such fees, charges and any other applicable fees and charges imposed by the Card Scheme. Such fees and charges will be debited from your settlement account in addition to the Chargeback.

Sample Chargeback Reasons

The following outlines the most common types of Chargebacks. This list is not exhaustive. We have included recommendations on how to reduce the risk of Chargebacks. These are recommendations only and do not guarantee that you will eliminate Chargebacks.

Chargebacks Due to Authorisation Description

Proper Authorisation procedures were not followed and valid Authorisation was not obtained.

Likely Scenario

- Authorisation not obtained
- Authorisation was declined
- Transaction processed with an expired Card and Authorisation was not obtained
- Transaction processed with an invalid account number and Authorisation was not obtained

Recommendations to Reduce Risk of Chargeback

- Obtain valid Authorisation on the day of the Transaction
    - If you receive a decline response, request another form of payment

Chargebacks Due to Cancellation and Returns Description

Credit was not processed properly or the Cardholder has cancelled or returned items.

Likely scenario

- Cardholder received damaged or defective merchandise
- Cardholder continued to be billed for cancelled recurring Transaction
- Credit Transaction was not processed

Recommendations to Reduce Risk of Chargeback

- Issue credit to the Cardholder on the same account as the purchase in a timely manner
- Do not issue credit to the Cardholder in the form of cash, cheque or in-store/merchandise credit as we may not be able to recoup your funds if the Transaction is charged back
- For recurring Transactions ensure customers are fully aware of the conditions
    - Cancel recurring Transactions as soon as notification is received from the Cardholder or as a Chargeback, issue the appropriate credit as needed to the Cardholder in a timely manner; and
- Provide proper disclosure of your refund policy for returned/cancelled merchandise or services to the Cardholder at the time of Transaction. Card present, Cardholder signed the sales draft containing disclosure
- For e-commerce, provide disclosure on your website on the same page as checkout
- Ideally have the Cardholder to click to accept prior to completion

Chargebacks Due to Fraud Description

Transactions that the Cardholder claims are unauthorised; the account number is no longer in use or is fictitious, or the merchant was identified as “high risk.”

Note: For Visa Transactions, to ensure that you preserve your Chargeback rights, you must:

- Complete a retrieval request and provide a sales slip that contains all required data elements; and
- Respond to all retrieval requests with a clear legible copy of the Transaction document that contains all required data elements within the specified timeframe

Likely Scenario

- Multiple Transactions were completed with a single Card without the Cardholder’s permission
- A counterfeit Card was used and proper acceptance procedures were not followed
- Authorisation was obtained; however, full track data was not transmitted
- The Cardholder states that they did not authorise or participate in the Transaction

Recommendations to Reduce the Risk of Chargeback Card Present Transactions

- Obtain an Authorisation for all Transactions
- For recurring Transactions ensure customers are fully aware of the conditions
- Cancel recurring Transactions as soon as notification is received from the Cardholder or as a Chargeback, and issue the appropriate credit as needed to the Cardholder in a timely manner
- You should avoid keying the Card data into your terminal unless you have been given Mail Order/Telephone Order (MO/TO) access and permission to do so

Recommendations to Reduce the Risk of Chargeback Card-Not-Present Transactions

- Ensure delivery of the merchandise or services ordered to the Cardholder
- Participate in recommended fraud mitigation tools
  - Verified by Visa Program
  - Mastercard SecureCode

Note: While Transactions utilising these tools may still be disputed; the service may assist you with your decision to accept certain Cards for payment.

- Obtain Authorisation for all Transactions
- Ensure merchant descriptor matches the name of the business and is displayed correctly on the Cardholder statement
- Ensure descriptor includes correct business address and a valid customer service number

Chargebacks Due to Cardholder Disputes Description

Goods or services not received by the Cardholder, merchandise defective or not as described.

Likely Scenario

- Services were not provided or merchandise was not received by the Cardholder
- Cardholder was charged prior to merchandise being shipped or merchandise was not received by agreed upon delivery date or location
- Cardholder received merchandise that was defective, damaged or unsuited for the purpose sold or did not match the description on the Transaction documentation/verbal description presented at the time of purchase
- Cardholder paid with an alternate means and their Card was also billed for the same Transaction
- Cardholder cancelled service or merchandise and their Card was billed
- Cardholder billed for a Transaction that was not part of the original Transaction document
- Cardholder claims to have been sold counterfeit goods
- Cardholder claims the merchant misrepresented the terms of sale

Recommendations to Reduce Such Risk of Chargeback

- Provide services or merchandise as agreed upon and described to the Cardholder; clearly indicate the expected delivery date on the sales receipt or invoice
- Contact the Cardholder in writing if the merchandise or service cannot be provided or is delayed, and offer the Cardholder the option to cancel if your internal policies allow
- If the Cardholder received defective merchandise or the merchandise received was not as described; resolve the issue with the Cardholder at first contact
- If the merchandise is being picked up by the Cardholder, have them sign for the merchandise after inspecting that it was received in good condition
- If unable to provide services or merchandise, issue a credit to the Cardholder in a timely manner

- Accept only one form of payment per Transaction. Ensure the Cardholder is only billed once per Transaction
- Do not bill Cardholder for loss, theft or damages unless authorised by the Cardholder
- Ensure that a description of the service or merchandise provided is clearly defined

Chargebacks Due to Processing Errors Description

Error was made when Transaction was processed or it was billed incorrectly.

Likely Scenario

- The Transaction was not deposited within the Card Scheme specified timeframe
- The Cardholder was issued a credit however the Transaction was processed as a sale
- The account number or Transaction amount used in the Transaction was incorrectly entered
- A single Transaction was processed more than once to the Cardholder's account
- The Cardholder initially presented the Card as payment for the Transaction. However, the Cardholder decided to use an alternate form of payment.

Recommendations to Reduce Risk of Chargeback

- Process all Transactions within the Card Scheme specified timeframes
- Ensure all Transactions are processed accurately and only one time
- If a Transaction was processed more than once, immediately issue voids, Transaction reversals or credits
- Ensure that credit Transaction receipts are processed as credits and sale Transaction receipts are processed as sales
- Ensure all Transactions received a valid Authorisation approval code prior to processing the Transaction
- Do not alter Transaction documentation or make any adjustments unless the Cardholder has been contacted and agrees to modifications of the Transaction amount
- Retain copies of all Transaction documentation for the required timeframe that is specified by each Card Scheme
- Develop efficient methods to retrieve Transaction documentation to maximise ability to fulfil requests
- Merchant should retain the Transaction documents for 13 months from the date of Transaction

11. Suspect/Fraudulent Transactions

If the Card being presented or the behaviour of the person presenting the Card appears to be suspicious or you otherwise suspect fraud, you must immediately contact the Fiserv Customer Support Hotline listed on Page 2 of this Guide.

While not proof that a Transaction is fraudulent, the following are some suggestions to assist you in preventing fraudulent Transactions that could result in a Chargeback

Does the Cardholder:

- Appear nervous/agitated/hurried?
- Appear to be making indiscriminate purchases (for example, does not care how much an item costs, the size and so on)?
- Make purchases substantially greater than your usual customer (for example, your average Transaction is $60, but this Transaction is for $360)?
- Insist on taking the merchandise immediately (for example, no matter how difficult it is to handle, is not interested in delivery, alterations and so on)?
- Appear to be purchasing an unusual amount of expensive items or the same items?
- Talk fast or carry on a conversation to distract you from checking Authorisation code obtained or where applicable, the signature?
- Take the Card from a pocket instead of a wallet?
- Repeatedly come back, in a short amount of time or right before closing time, to make additional purchases?
- Cause an unusual, sudden increase in the number and average sales Transactions over a one-to three-day period?

Does the Card:

- Have characters the same size, height, style and all within alignment?
- Appear to be re-embossed (the original numbers or letters may be detected on the back of the Card)?
- Have a hologram? Does it look damaged? Never accept a Card without the hologram

- Have a Chip?
- Have a magnetic stripe on the back on the Card?
- Have an altered signature panel (for example, appear discoloured, glued or painted or show erasure marks on the surface)?
- Have “valid from” (effective) and “valid thru” (expiration) dates consistent with the sale date?

We also recommend that you are vigilant for any Cardholder who behaves as follows, specifically in relation to prepaid Cards:

- Frequently makes purchases and then returns the goods for cash
- Uses prepaid Cards to purchase other prepaid Cards
- Uses large numbers of prepaid Cards to make purchase

12. Dynamic Currency Conversion (DCC)

- Disclosures must happen when Dynamic Currency Conversion is offered and before the Cardholder is prompted to actively choose the Transaction currency
- Merchants must utilise screens and/or receipts that are deemed compliant by the Cards associations in order to offer Dynamic Currency Conversion
- As part of your initial implementation of Dynamic Currency Conversion your screens and receipts will be reviewed for compliance purposes by our Dynamic Currency Solutions Product Team. Additionally, any future changes to screens and/or receipts need to be reviewed by the Global Currency Solutions Product Team to ensure continued compliance with Card Scheme Rules.
- There are explicit rules related to offering Dynamic Currency Conversion when utilising customer facing devices. Specifically:
    - Offer cannot contain YES/NO buttons. They may instead provide the offering in a neutral manner such as “Pay in EUR”/“Pay in USD”
    - Offers cannot utilise different colored selection buttons such as RED/GREEN
    - Offer cannot utilise different font size or bold characters

Steering

- It cannot be said often enough: The merchant must never steer a Cardholder to choose Dynamic Currency Conversion over the merchant’s base currency
- Based on guidance from the Card Schemes, steering can occur in many forms and are not necessarily obvious to merchants or their sales staff. Steering can appear as active or passive, but neither is permitted

In general, merchants should utilise caution and be aware of the following regulations when offering Dynamic Currency Conversion:

- The merchant must not use any language or procedure that would cause the Cardholder to choose Dynamic Currency Conversion by default
- The merchant must not us any language or procedure that may make paying in the merchant’s local currency difficult to understand
- The Cardholder must consent to opt in for each Dynamic Currency Conversion Transaction. Although for certain vertical markets such as travel and entertainment expenses, merchants may capture the Cardholder’s decision in advance and utilise this during their hotel stay, cruise trip or car rental.

13. Glossary

- **Application**: The agreement between the Merchant and Fiserv Merchant Solutions comprising the Merchant Application and any supporting documents each as amended from time to time
- **Authorisation:** The confirmation by the Issuer that the Card number exists and that enough funds are available to allow the Transaction to go ahead
- **Authorisation Approval Code**: A number issued to a participating merchant which confirms the authorisation for a sale or service
- **Card**: A payment card or any form factor that can be used to initiate a payment Transaction as specified on the Application
- **Cardholder**: Means the individual whose name is embossed on a Card and any authorised user of such Card
- **Card Scheme**: Any entity formed to administer and promote Cards, including without limitation Mastercard International, Inc, Visa International, Inc and UnionPay International
- **Card Scheme Rules**: The rules, regulations, releases, interpretations and other requirements (whether contractual or otherwise) imposed or adopted by any Card Scheme
- **Card Validation Value**: A three-digit value printed in the signature panel of most Cards. Visa's Card Validation Code is known as CVV2; Mastercard's Card Validation Code is known as CVC2. Card Validation Codes are used to deter fraudulent use of an account number in a non-face-to-face environment, For example, MOTOs and Internet orders), which must not be stored after Authorisation
- **Chargeback**: The reversal of a sales Transaction (or other indicia of a Card Transaction) and reversal of any associated credit to your funding/settlement account because a Cardholder or Issuer disputes the Transaction or can be reversed under associated operating procedures
- **Chip:** An microprocessor embedded Cards which stores and protects Cardholder data
- **Credit Card**: A valid Card bearing the service mark of Visa, Mastercard (and any other Card agreed by the parties), the use of which accesses the Cardholder's credit facility or a debit facility through one of the Card Schemes
- **Credit Receipt**: A document evidencing the return of merchandise by a Cardholder to a merchant or other Refund made by the merchant to the Cardholder
- **Debit Card**: A valid Card the use of which accesses the Cardholder's cheque or savings account facility made available by the Issuer
- **EMV**: Chip technology standards originally developed by Europay, Mastercard and Visa where data is stored on integrated circuits rather than a Magnetic Stripe
- **Issuer**: Cardholder's bank or the bank, which has issued a Card to an individual
- **Magnetic Stripe**: A stripe of magnetic information affixed to the back of a plastic Card
- **Merchant**: The party identified as "Merchant" in the Merchant Agreement. The words "you" and "your" refer to Merchant
- **Refund**: The reversal of a sales Transaction in accordance with the Merchant Agreement
- **Transaction**: Includes a sales transaction (being the supply of goods or services or both), a cash out transaction, Refund or Cash Related transaction in which a Card or Card number is used and which is processed by the Merchant either manually or electronically