Your payment acceptance guide

Spenda Business Services Pty Ltd

Welcome

From start to finish

A Guide to Accepting Payments

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 this guide on how to accept payments. It's your quick reference to the guidelines for processing transactions. You'll also find recommendations and tips to help you prevent fraud, reduce chargebacks, and properly handle payments, refunds, exchanges, and most other situations you'll encounter in your day-to-day business.

If you have questions about processing payments or other aspects of your merchant arrangement, please contact our customer success team on 1300 682 521.

Contents

Part I

General

Spenda Business Services Pty Ltd (Spenda) provides processing services to facilitate the passage of your Sales Receipts back to the thousands of institutions that issue the cards carried by your customers.

This part of the Guide describes the procedures and methods for submitting Card Scheme transactions for payment, obtaining authorisations, responding to chargebacks and media retrieval requests, and other aspects of the operations of our services.

They seek to provide you with the principles for a sound card program. They are designed to 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, eftpos Australia and UnionPay. In the event Spenda provides authorisation, processing or settlement of transactions involving other Card Scheme brands, you should also consult those independent Card Schemes to acquaint yourself with 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 State or Territory.

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

Use of Card Scheme Brands

Do's

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

Don'ts

- Don't indicate that Spenda 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 Spenda or of the Card Schemes in any way that injures or diminishes the goodwill associated with the trademarks
- Don't use our trademarks of Spenda or the Card Schemes in any manner, including in any advertisements, displays or press releases, without our prior written consent

Validating Card Brands

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

Additionally, Spenda has made provision for the acceptance and on-forwarding of transactions for American Express®, Diners® and JCB. You will need to engage these Card Schemes separately for contractual arrangements which will include processing, funding and providing you a statement.

Merchant Statements

Each month Spenda will send you a statement. The statement will reflect all activity for the month. The statement will also include a table reflecting the cost of acceptance of these transactions as required under law.

- Review your statement carefully and if you have any questions, please contact our customer success team on 1300 682 521
- Familiarise yourself with Cost of Acceptance requirements and guidelines as stipulated by the Reserve Bank of Australia (RBA) and the Australian Competition and Consumer Commission (ACCC)

Point of Sale (POS) Reminders

You must clearly and conspicuously:

- Disclose all material terms of sale 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

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/telephone MO/TO), Internet/eCommerce.

You may only conduct eCommerce 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

Do's

- Do obtain the card account number, name as it appears on the card, expiration date of the card and the cardholder's statement address
- Do notify the cardholder of delivery time frames and special handling or cancellation policies
- Do 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 eCommerce, do add a "tick box" or acceptance confirmation so the cardholder acknowledges the terms

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

Transaction Guidelines

Do's

- Do only present for payment valid charges that arise from a transaction with a bona fide cardholder

- Do ensure transaction amounts reflect the inclusion of Goods and Services Tax (GST)
- Do disclose any surcharge to be applied

Don'ts

- Don't set a minimum transaction amount for any Card Scheme cards including cards bearing the eftpos Australia symbol
- Don't set a maximum transaction amount for any Card Scheme cards or cards bearing the eftpos Australia symbol
- 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 bearing the eftpos Australia symbol
- 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 for the likes of 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

Security

You are responsible for maintaining the security of your POS devices, particularly if the device is the asset of Spenda 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:

Do's

- Do install and maintain a secure firewall configuration to protect data
- Do protect stored data, and do encrypt the 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
- Do use and regularly update anti-virus software and keep security patches up-to-date
- Do 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
- Do regularly test security systems and processes
- Do maintain a policy that addresses information security for employees and contractors
- Do restrict physical access to cardholder information
- Do destroy or purge all media containing obsolete transaction data with cardholder information
- Do 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
- Do 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 cardholder 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

Gives You Helpful Information and Guidelines for Specific Aspects

This part of the *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 Call Centre with any questions that arise as you review this information.

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 approval of the sale from other sources. Instead, request another form of payment
- 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 EFTPOS terminal to obtain an authorisation approval code
- Follow the prompts on the EFTPOS 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.

EFTPOS Debit Cards and Multi-Network Cards

Acceptance

EFTPOS Debit Cards are cards that bear the EFTPOS logo and can be used for card present transactions in Australia only. Multi-Network cards are Scheme issued debit cards but which may also bear the EFTPOS logo and operate as an EFTPOS Debit Card. These cards can be accepted where properly authorised to do so. If the Debit Card/ Multi-Network Card is valid, you must comply with the following general requirements:

- You must honour all valid Debit Cards and Multi-Network Cards when presented that bear authorised network marks and/or the EFTPOS logo
- You must treat transactions by cardholders from all issuers in the same manner
- You may not establish a minimum transaction amount for Debit Card acceptance
- A signature is not required for debit account (cheque or savings) transactions

- You shall not disclose transaction-related information to any party other than your agent, a debit card network, or issuing institution and then only for the purpose of settlement or error resolution
- You may not process a Credit Card transaction in order to provide a refund on a Debit Card transaction

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) and by the cardholder 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, the 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 EFTPOS 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 so as to prevent unauthorised access, use or disclosure

Cash out from purchase

- You have the option of offering cash out to your customers when they make a debit account purchase
- You may set a minimum and maximum amount of cash out that you will allow
- If you are not now offering this service, your terminal may require additional programming to begin offering cash out

Adjustments

An adjustment is a transaction that is initiated to correct a Debit Card/Debit Account transaction that has been processed in error. You will be responsible for all applicable adjustment fees that may be charged by.

There are several reasons for adjustments being initiated:

- The cardholder was charged an incorrect amount, either too little or too much
- The cardholder was charged more than once for the same transaction
- A processing error may have occurred that caused the cardholder to be charged even though the transaction did not complete normally at the POS

All parties involved in processing adjustments are regulated by time frames that are specified in the operating rules of eftpos Australia Limited, ePayments Code and other applicable laws.

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.

Do's

- Do execute two separate transactions and obtain an authorisation for each on each transaction date
- Do 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
- Do obtain proof of delivery upon delivery of the services/ merchandise purchased

Don't

- 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.

Do's

- Do 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
- Do obtain an authorisation for each transaction
- Do 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 Spenda 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.

Do's

- 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

Refunds

Do's

- For eCommerce, 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 fulfilling the checkout
- Do 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.

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
- If you do receive a chargeback, investigate and if you dispute the chargeback, submit the appropriate documentation within the required time frame
- Whenever possible, contact the cardholder directly to resolve the dispute
- If you have any questions, call the Call Centre

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 time frame 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 and 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, and issue the appropriate credit as needed to the cardholder in a timely manner
- 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 eCommerce, 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 time frame

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
- If you are utilising an EFTPOS terminal to capture card data, present all card transactions through your EFTPOS terminal to capture cardholder information
- You should avoid keying the card data into your EFTPOS 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 time frame
- 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 time frames
- 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 time frame that is specified by each Card Scheme
- Develop efficient methods to retrieve transaction documentation to maximise ability to fulfil requests



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 customer success team on 1300 682 521.

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 purchases

Glossary

Application: The agreement between the Merchant, First Data Merchant Solutions Australia Pty Ltd. and Spenda Business Services Pty Ltd. comprising the merchant application and any supporting documents each as amended from time to time.

Authorisation: The confirmation by the card 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, eftpos Australia Limited, 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, MO/TOs 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 card issuer disputes the transaction or can be reversed under associated operating procedures.

Chip: A 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 cardholder's issuer.

EMV: Chip technology standards originally developed by Europay, Mastercard and Visa where data is stored on integrated circuits rather than a magnetic stripe.

ePayments code: The ePayments code developed by the Australian Securities and Investment Commission.

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" on the application. The words "you" and "your" refer to merchant.

Refund: The reversal of a sales transaction in accordance with the operating procedures.

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.