Merchant chargeback and fraud protection guide

Spenda Business Services Pty Ltd

Contents

Introduction 2

What is a chargeback? 3

Most common reason for chargebacks? 3

How does Spenda notify me when a Chargeback has been filed against me? 4

What is the chargeback/ dispute process? 4

What evidence can I provide to support my chargeback dispute? 6

Best practices for avoiding chargebacks 7

Card present credit card fraud 9

Chip card processing 10

Card-not-present credit card fraud 10

Common indicators of fraud 11

Refund fraud 13

A merchant's website responsibilities 13

Money laundering 14

Securing your EFTPOS terminal 14

Recommended best practices 14

Contact us 15

Introduction

At Spenda Business Services Pty Ltd. (Spenda), protecting our customers against Chargebacks and Fraud is of the utmost importance to us.

Fraud can cost your business significant amounts of money, and certain types of merchants – based on the types of goods or services sold – are more at risk of fraudulent transactions than others.

We believe it is essential for you to have a sound understanding of credit card fraud, how it can be detected and how it can be prevented. We have prepared this guide to give you a range of precautions and advice you can take to minimise these risks and continue to do business confidently and prosperously.

Please keep a copy handy as a reference and you can also find a copy on the Spenda Website.

What is a chargeback?

A Chargeback is a reversal of a card transaction and usually occurs when a cardholder raises a dispute with their financial institution (also known as the Issuer) in relation to a purchase made with their credit or debit card.

The processing and investigation of Chargebacks is governed by the Schemes (i.e., Visa, MasterCard or American Express). This includes timeframes, transaction processing requirements and the acceptable documentation that banks and acquirers (such as Spenda) must submit.

A Chargeback may result in the amount of the original sale and a Chargeback fee to be deducted from the merchant's account. The reasons why Chargebacks occur may vary, however, they are generally the result of customer dissatisfaction with their purchase or because of unauthorised or fraudulent use of their card.

Most common reason for chargebacks?

Chargeback reason	Why has this happened?
Unauthorised/Fraudulent Transaction	Cardholder does not recognise the transaction. This can occur when a cardholder does not recognise your trading name on your credit card statement. Tip: You should always trade under the same name you have provided for your merchant facility and ensure it appears on your transaction receipts.
Processing Error	Cardholder/Issuer believes transaction has been processed incorrectly. Common scenarios include: • Incorrect transaction amount/card number • Late presentment of the transaction
Duplicate/Multiple Processing	Cardholder claims transaction for same goods/services was processed more than once.
Non-receipt of Goods/Services	Cardholder claims goods/services for the transaction has not been received/rendered to the agreed-upon location or by the expected delivery date.

How does Spenda notify me when a Chargeback has been filed against me?

When Spenda is notified that a cardholder has filed a Chargeback against you, we send an email to the address that you nominated for financial notifications. It's important that you check this email address on a regular basis.

What is the chargeback/ dispute process?

1. The cardholder lodges a dispute with their card issuer/bank.

2. The bank sends a Retrieval Request to Spenda.

3. Spenda sends an email to your nominated email for financial notifications, requesting a copy of the EFTPOS receipt or a tax invoice in case of MOTO (Mail Order/Telephone Order) * transactions.

   It's important that you respond to us promptly. Failure to respond within the specified timeframe (usually eight days) may result in the value of the transaction being charged back to you.

4. If the cardholder's bank is not satisfied with the response, they may initiate a Chargeback and a debit for the Chargeback amount is applied to your bank account. If this happens, we will also notify you via email. Please note, a Chargeback fee will be charged at the end of the month.

5. Spenda sends an email to your nominated email address for financial notifications, requesting additional documentation to represent the Chargeback. Again, it's important that you respond within the specified timeframe (usually eight days).

6. Spenda represents the chargeback to the cardholder's bank using the documentation submitted by you.

7. If, once the documentation you supplied is reviewed and the Chargeback is ruled in your favour, we will credit your settlement account with the Chargeback amount. The Chargeback fee will not be refunded.

It should be noted that not all retrieval requests will result in Chargebacks. Further, it should be noted that all Chargebacks do not need to be preceded by retrieval requests.

The cardholder's bank is entitled to Chargeback a transaction even if a retrieval request has not been made.

There are two ways you can send us evidence:

Email: merchantservices@spenda.co

Post: Att. Merchant Services, Spenda Business Services Pty Ltd., 605, 275 Alfred Street, North Sydney, NSW, 2060

One of our Chargeback specialists will combine the evidence provided by you with any other information Spenda may already have and dispute the Chargeback where appropriate.

What evidence can I provide to support my chargeback dispute?

Evidence required to refute the Chargeback:	You may be liable for Chargebacks if:
Receipts for all card-present transaction by the required timeframes.	The transaction processed was manual/card not present and all surrounding information including one or more of the following: • If your response is not received within the specified timeframe.
Transaction receipt and all other related documentation to prove the transaction was processed: • With a payment by other means • Within the mandatory time limit • With correct transaction amount/card number	No legible transaction receipt and documentation is provided to prove the transactions were processed accurately.

Evidence required to refute the Chargeback:	You may be liable for Chargebacks if:
• Two separate transaction receipts or other records to validate separate transactions. • Documentation to show that a refund was processed to offset the disputed transaction through the same payment channel the cardholder used to make the original payment.	You are unable to provide evidence to support separate transactions. You accidentally processed the same transaction twice or more for the same purchased goods and/or services. You did not process a refund via the same payment channel as the disputed transaction.
Signed documentation to prove that the cardholder or cardholder authorised recipient received the merchandise/service by the expected delivery date and at the agreed location.	Goods and/or services were not received by the appropriate recipient at the agreed location by the expected delivery date. You are unwilling or unable to provide the goods/services and have not refunded the cardholder via the same payment channel as the disputed transaction.

Best practices for avoiding Chargebacks

- Use a clear trading name on your receipts that the customer will recognise.
- Make every effort to know your customer and to respond promptly to any customer service requests.
- Keep records about the transaction and your customer, including email or other correspondence.
- Respond promptly to requests for EFTPOS receipts and Chargebacks.
- Provide legible documentation when responding to retrieval requests, ensuring you can see the truncated card number, transaction date and transaction amount.
- Quickly process refunds for your customers using the same card used for the original sale and avoid refunding via cash or cheque if the purchase was made on a credit/debit card.
- Make sure your customer is aware of a cancellation or refund policy in writing and have your refund/cancellation policy clearly printed on the transaction receipt in close proximity to the signature line. It should also be stated on your website and in store. If you do not offer refunds or only offer in-store credit, this information should be included on your transaction receipt.
- Disclose all Terms and Conditions to the cardholder at the time of purchase. These should be clear and concise and should be acknowledged by the customer by signature or initials if the customer is present or available during the order process and for online orders, if they require a "Click to Accept".
- Always get signed proof of delivery and for delayed delivery make sure you get a signature from the cardholder at point of delivery.
- Do not accept declined transactions. Note: Do not split a declined transaction into smaller amounts to avoid authorisation, as this may result in a Chargeback.
- Card Present Transactions: Dip or tap the customer's credit card through your terminal and ensure you obtain a signature from the cardholder for transactions where required. DO NOT MANUALLY ENTER THE CARD NUMBER – instead, ask the cardholder for a different card.

- Card Not Present Transactions (MOTO)*: Obtain as much information about the cardholder as possible. This can include full name, address, phone numbers, email address, credit card number, name of bank, expiry date, CCV, company name etc.

- Verify the name and address in the phone directory or via Google if the transaction appears unusual. It is advisable to obtain the cardholder's signature on some correspondence, e.g., an order confirmation.

- Communicate with customers to try to establish mutually satisfactory solutions to problems relating to the quality of goods or services provided.

- Verify the details of customers placing large or suspicious orders.

- Only charge the customer's account when the goods are shipped. If a delayed delivery is required, wait to process the transaction until goods are shipped.

- Exercise caution when taking foreign orders. Orders from Asia, the Middle East, Eastern Europe and Africa may represent a higher risk.

* Be aware that the risk with all MOTO transactions (i.e., card not present) resides with you, the merchant, not the bank/acquirer or the cardholder.

Card present credit card fraud

Before you start a transaction, check that:

- You're authorised to accept the card
- The card does not appear to be damaged or altered Check on the front of the card that:
    - The name on the card is appropriate to the customer (e.g., a man presenting a card with a woman's name should be questioned)
    - The printing on the card looks professional
    - The card has current validity dates (a card can only be used from the first day of the 'valid from' month to the last day of the 'until end' month)
    - If there is a hologram on the card, it does not appear suspicious or made of inferior material – it should look three-dimensional Check the embossing is:
    - raised, not flattened (unless it is an unembossed card)
    - clear and even
    - accurate, so that the first four digits of the embossed number match the pre-printed four digits on the card
- Be alert for customers acting suspicious or who:
    - Appear nervous, overly talkative or in a hurry
    - Arrive on closing time
    - Try to rush you or upset your concentration
    - Carry the card loose or by itself
    - Have no means of identification
    - Make numerous purchases under your Authorised Floor Limit (refer to your Merchant Agreement for more information)
    - Make purchases without regard to size, quality or price of goods
    - Ask for transactions to be split
    - Ask for transaction to be manually entered

Chip card processing

Chip cards are cards that are embedded with a security microchip that provides further protection to help lower the risk of fraudulent transactions and Chargeback disputes. Look at the card and if there is a chip, always insert the card into the chip reader at the first instance.

As with any other transaction, a degree of caution must also be exhibited when processing chip card transactions if:

- The terminal displays "Insert Chip" when the card is swiped through the terminal and the card in question does not have a chip on it, do not proceed with the transaction.
- The terminal displays "Insert Chip" and the chip – when inserted – cannot be read by the terminal, do not proceed with the transaction.

If you're suspicious of a transaction:

- Ask for photographic identification (e.g., a driver's licence or passport) and check that the details match the Cardholder's name appearing on the card.
- Record the details on your copy of the printed Transaction Voucher Don't risk it. If you remain suspicious about the transactions, refund the credit transaction and ask your customer for a direct deposit or some other form of payment (particularly for large value sales).

Card-not-present credit card fraud

Mail, Telephone and Internet Orders (MOTO)

Any credit card transaction where the card and/or cardholder is not present poses a higher risk to your business. Being vigilant about unusual spending or behaviour can help you identify early warning signals that something may not be right with an order.

While the following situations or scenarios may occur during a valid transaction, combinations of these may be cause for alarm.

Common sense and instincts should be your guide. Follow these security checks to minimise the risk of fraud and Chargebacks when processing card-not-present transactions involving mail, telephone or Internet (eCommerce) orders.

Common indicators of fraud

- Payments to a third party: When your customer requests a payment be made to a third party from the card payment to you, usually by Western Union Transfer, often disguised as a freight or logistics cost.
- Multiple card details: When multiple card details are presented, or multiple declines occur within a short period of time.
- Split transactions: When you are requested to split transactions over a number of cards.
- Large or unusual orders: When items are ordered in unusual quantities and combinations and/or greatly exceed your average order value.
- Email addresses: Be wary of customers using a free email service (i.e., yahoo, hotmail, gmail). This is a potential risk as they do not require a billing relationship or verification that a legitimate cardholder opened the account.
- Delivery addresses: Exhibit caution with orders that are being shipped to international destinations you may not normally deal with. Delivery to Post Office Boxes can also indicate potential fraud.
- Freight: orders requesting express freight can be a fraud indicator as they want to obtain the goods as quickly as possible.
- IP addresses: Record and check the IP address of your online customers – you may find their IP address is not in the same location they claim to be. However, it is important to note that sophisticated fraudsters often hide their IP address.
- Unlikely orders: Orders are received from locations where the goods or services would be readily available locally, or you receive an order for additional products that you do not normally see (i.e., Mobile Phones).
- Refund requests: Specifically, when orders are cancelled and refunds are requested via telegraphic transfer, Western Union Transfer, or to an account other than the card used to make the purchase.

- Numerous orders: A small value order followed by a large order a few days later can indicate possible fraud. Often, fraudsters will place a very small order to begin with, hoping this will not be questioned and go undetected. Once they know the first small fraud transaction has gone through, they will place orders for larger value goods hoping this still won't be questioned as they are now an established customer.

- Lack of customer details: e.g., no phone numbers, no residential address, etc.

- Phone order to be picked up: Be wary of customers wishing to pay for an item with credit card over the phone, but pick up the goods from your store, which lets them make the purchase without providing personal information (i.e., shipping, billing address), and the same card-not-present risks apply.

- When taking an order, as well as obtaining the credit card number, expiry date and full name, we recommend you also obtain the following:
    - Cardholder's physical address
    - Cardholder's contact phone numbers including landline contacts
    - The name of the Card Issuing Bank and the country the card was issued in

Good Advice:

Trust your instincts. If a sale seems too good to be true, it probably is. All too often what a merchant might think is a great sale will turn out to involve some type of fraud. Take the time to properly investigate overseas orders from customers with whom you have never done business. That bit of extra work may well prevent you from becoming the victim of a fraud scheme and having to bear any associated Chargebacks.

Refund fraud

Unfortunately, refund fraud through a merchant terminal can be quite common. Refund fraud involves employees processing refunds (credits) to their own credit or debit card via your EFTPOS terminal. Essentially, this is removing funds from your business' bank account and placing those funds into the employee's account.

Spenda have measures in place to help protect your business from this type of fraud.

Ways to safeguard against refund fraud include:

- Strictly controlling access to your EFTPOS terminal for authorised staff only
- Printing and checking your daily summary from the terminal to help identify large/unusual refunds
- Ensuring you change your Refund password regularly and limit who has access to the password
- Always balancing EFTPOS settlement and refunds

A merchant's website responsibilities

Make sure your website:

- Offers an accurate description of the goods and services you're selling
- Contains a clear explanation of shipping practices and delivery policy/timeframe
- Displays card logos wherever payment options appear
- Clearly states your refund/return policy and that your policy complies with the relevant consumer law
- Displays total cost of the goods or services purchased (including shipping charges)
- Contains all required contact details – trading name, address and Australian Business Number (ABN) where applicable
- Avoids cardholder confusion by making sure the URL and trading name are not significantly different
- Contains the security capabilities and policy for transmitting of payment card details
- Clearly outlines export restrictions
- Clearly explains your consumer data privacy policy, i.e. – what you do with any customer information you collect
- Provides individual payment pages for each merchant domain names and doesn't link to another website where payment is made for the goods or services offered on the originating site

Money laundering

Money laundering is a serious breach of your Merchant Agreement and exposes your business to major financial loss. Put simply, laundering involves a merchant processing transactions on behalf of another merchant.

Laundering is to be avoided at all costs, even if you're offered an attractive inducement such as a percentage of the transaction.

Securing your EFTPOS terminal

Your EFTPOS terminal is equipped with a number of built-in security features designed to protect your customers' information. By implementing the recommended best practices below, you can help protect your business, your customers and your reputation from credit and debit card fraud or misuse.

Recommended best practices

Always ensure that:

- Terminals are secure and under supervision during operating hours (including any spare or replacement EFTPOS terminals you have).
- Only authorised employees have access to your EFTPOS terminals and are fully trained on their use.
- Your EFTPOS terminals are securely locked and not exposed to unauthorised access when closing your store.
- Only authorised Spenda personnel are permitted to maintain, swap or remove your EFTPOS terminal, and always ensure that security identification is provided.
- Your EFTPOS terminal is never maintained, swapped or removed without notice from Spenda. Be aware of unannounced terminal service visits.
- You inspect your EFTPOS terminals on a regular basis and check that the terminal casing is whole with external security stickers remaining unbroken and of a high print quality.
- There are no additional cables running from your EFTPOS terminal .
- Your software is updated to the latest version.
- Any CCTV or other security cameras located near your EFTPOS terminal(s) cannot observe Cardholders entering details.

Notify Spenda Merchant Services on **1300 682 521** immediately if:

- Your EFTPOS terminal is missing
- You, or any member of your staff, is approached to perform maintenance, swap or remove your EFTPOS terminal without prior notification from Spenda and/or Security Identification is not provided
- Your EFTPOS terminal prints incorrect receipts or has incorrect details
- Your EFTPOS terminal is damaged or appears to be tampered with

Contact us

Phone: 1300 682 521
Email: merchantservices@spenda.co
Online: spenda.co/merchant-services/