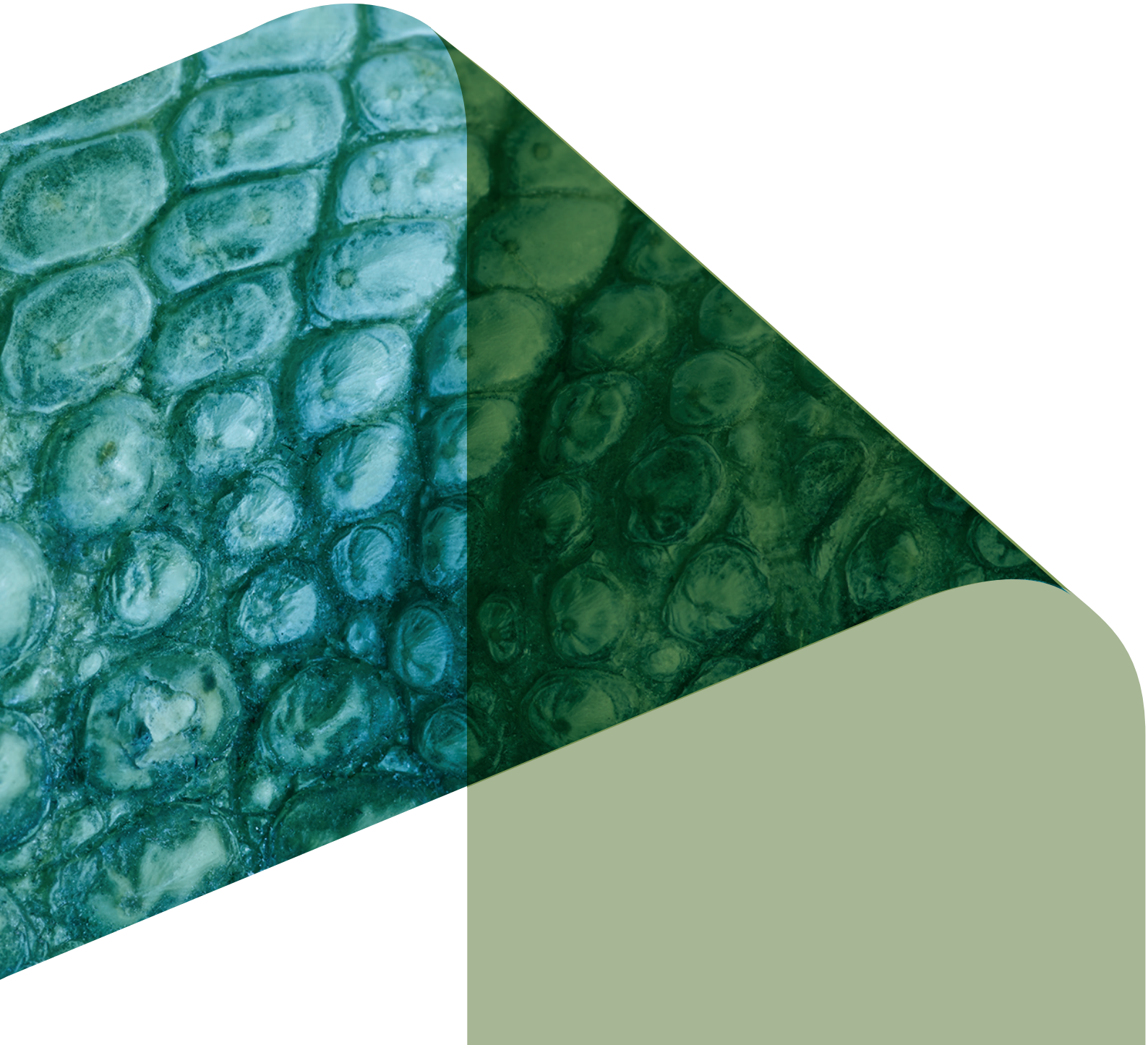
BOQ SPECIALIST
Distinctive banking

Your Merchant Facility and Managing Risk



How to Minimise Disputes, Chargebacks and Fraudulent Transactions

We want to help you get the most out of your merchant facility and provide a secure and convenient payment method for you and your customers.

This guide will provide you with information to assist in understanding disputes, chargebacks and fraud risks associated with operating a merchant facility.

Dispute

What is a dispute?

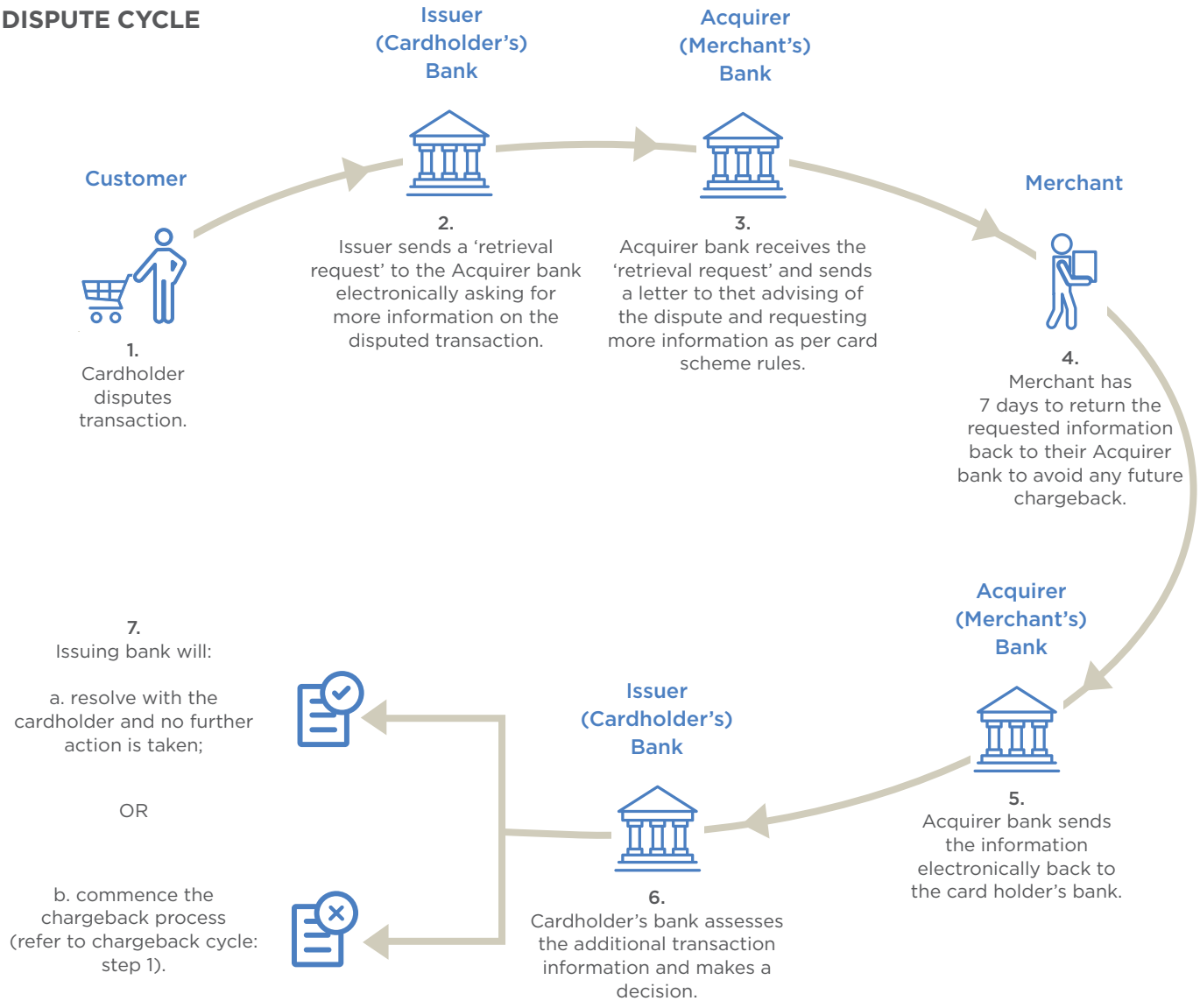
Dispute is a term used when a merchant's customer (cardholder) queries a transaction appearing on their card statement. The merchant will receive a letter from BOQ advising details of the disputed transaction and the information required by you to provide back to BOQ within a set timeframe.

This request from the customer's bank is only for information / documentation, it is not for value.

Below are some of the reasons why a cardholder or Issuing Bank will initiate a dispute:

- Transaction not recognised;
- Goods or services were never received;
- The cardholder did not authorise the transaction (card not present – fraudulent); or
- A transaction was processed twice by the merchant.

DISPUTE CYCLE



How does the dispute process work?

The card schemes (Visa and MasterCard) have set rules for all members (Card Issuers & Merchant Acquirers) globally to follow.

Dispute process steps:

1. Cardholder contacts their Bank advising an issue with a transaction appearing on their card statement or the Issuing Bank (Issuer) will set in motion the dispute process when a counterfeit card has been used;
2. The customer's Issuing Bank creates and sends a 'retrieval request' to BOQ requesting more information from our merchant on behalf of their customer;
3. BOQ sends you, the merchant, a letter requesting specific information / documentation to assist with your customer's investigation;
4. You are required to respond back to the address provided on the 'retrieval request' letter within the stated timeframe;
5. BOQ will assess to ensure the request for information / documentation has been fulfilled by you and will send this back to your customer's Issuing Bank;
6. The customer's Issuing Bank assess the information provided and contacts the cardholder regarding the received information; and
7. Both your customer's Issuing Bank and your customer make a decision to either accept the transaction charge or proceed with a chargeback.

Chargeback

What is a chargeback?

'Chargeback' is a term used when a card transaction is reversed and your nominated settlement account is debited with the amount of the sale.

Generally, if a cardholder disputes a transaction and you don't have sufficient evidence to show that the cardholder authorised the transaction, then you will be liable for the chargeback. For this reason, it is important that your business keeps good records to enable adequate investigation of any card transaction dispute and to assist with reduction of the risk of unnecessary chargebacks occurring.

The most common reasons for chargebacks include:

- Customer disputes;
- Fraud; and
- Processing errors by either the merchant or their Bank.

Chargeback timeframes

Chargebacks can take place up to 180 days from the date of the transaction being disputed.

What are the most common chargebacks?

Transaction not recognised by cardholder

Definition: The cardholder (merchant's customer) contacted their Bank (Issuer Bank) to lodge a dispute stating that they did not recognise a particular transaction appearing on their card statement. This means they do not recognise the merchant's name and/or location.

The 'retrieval request' (dispute) did not resolve the issue. The cardholder's bank creates and processes the chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale).

Hints on how to minimise this type of chargeback

Where possible always respond to a 'retrieval request' with the required documentation. This will automatically reduce the number of chargebacks where the cardholder does not recognise the merchant's name and / or location; and

The merchant's name is the single most important factor in the cardholder's recognition of the transaction appearing on their card statement. Therefore it is critical that the merchant name, while reflecting the merchant's 'Doing Business As' name, also be clearly identifiable to the cardholder. The merchant will need to supply more information around their merchandise, location and items the cardholder purchased.

Goods / Services not provided by Merchant

Definition: The cardholder (merchant's customer) contacts their Bank (Issuer) to lodge a dispute advising merchandise / service had not arrived from the merchant by the expected delivery date.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated settlement account is debited with the amount of the sale).

Hints on how to minimise this type of chargeback

Goods / Services delivered:

- Send to BOQ evidence of the delivery, such as a delivery receipt signed by the cardholder or a carrier's confirmation that the merchandise was delivered to the correct address

Delivery date has not expired:

- Send a copy of the transaction receipt to BOQ pointing out that the delivery date has not yet expired

Delayed delivery of merchandise:

- If the delivery of the merchandise is to be delayed, notify the customer of the delay and the expected delivery date. As a service to your customer, provide the customer the option of proceeding with the transaction or cancelling it. Send copies of this correspondence to BOQ for assessment.

Cardholder did not authorise – card not present (Mail Order / Telephone Order - MOTO) transaction

Definition: The cardholder (merchant's customer) contacted their Bank (Issuer Bank) to advise they did not authorise a 'card not present' (MOTO) transaction appearing on their card statement. There could be several reasons for not recognising the transaction:

- Cardholder did not recognise the merchant's name as it is different to the shop name; or
- Cardholder did not authorise or participate in the transaction.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale).

NB: An authorisation obtained on a fraudulent / counterfeit card only confirms that the funds were available at the time of the transaction. This authorisation does not confirm that the cardholder is the one making the transaction and therefore can result in a chargeback to the merchant, and at times, the loss of either goods or services.

Hints on how to minimise this type of chargeback

Cardholder did not recognise the merchant's name:

- The merchant's name is the single most important factor in the cardholder's recognition of the transaction appearing on their card statement. Therefore it is critical that the merchant name, while reflecting the merchant's 'Doing Business As' name, also be clearly identifiable to the cardholder. The merchant will need to supply more information around their merchandise, location and items the cardholder purchased.

Cardholder did not authorise or participate in the transaction – fraudulent / counterfeit transaction:

- Where possible the merchant should obtain the CVV2 from the cardholder (the 3 digit security number on the back of the card) – this helps validate that the customer is in possession of the card at the time of an order (it still however, might not mean the genuine cardholder is the one making the purchase);
- Be aware of urgent requests for quick or overnight delivery from the customer, as it can be a sign for possible fraud;
- Be aware of customers who are ordering above your usual transaction size and don't care about additional costs that may be involved;
- Customer has asked for goods to be delivered to a Post Office box.

Credit not processed by merchant

Definition: The cardholder (merchant's customer) contacts their Bank (Issuer Bank) acknowledging participation in a transaction for which goods were returned or services cancelled, but the credit has not appeared on their card statement.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale)

Hints on how to minimise this type of chargeback

- Always refund a sale value to the same card that the transaction was originally processed on, and retain evidence of the refund processed.
- Never process a refund, direct to a Bank account, by cash or by other means.

Cancelled Recurring Transaction

Definition: The cardholder (merchant's customer) contacts their Bank (Issuer Bank) to notify that they have cancelled a recurring transaction however it is still appearing on their card statement.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale).

Hints on how to minimise this type of chargeback

- Always process the cancellation in a timely manner.
- Send notification to the cardholder advising the cancellation request has been processed.

Fraud/Counterfeit Cards/Skimming

What is a fraudulent transaction?

A fraudulent transaction occurs when a card account is used through the theft of the account holder's card number and card details. This can occur in several ways:

- Stolen / lost card; and
- Counterfeit cards (mainly created via skimming).

NB: An authorisation obtained on a fraudulent / counterfeit card only confirms that the funds were available at the time of the transaction. This authorisation does not confirm that the cardholder is the one making the transaction and therefore can result in a chargeback to the merchant, and at times, the loss of either goods or services.

Hints on how to minimise fraudulent transaction

- Where possible for all MOTO transactions obtain the CVV2 3 digit number
- Recognise suspicious orders, such as:
  - Transaction requests that are above your average purchase value;
  - Delivering to overseas addresses;
  - Customers who do not care what the value of the purchase is or additional costs (such as shipping / postage);
  - Delivery to post office boxes;
  - Rushed request where the cardholder advises they needed to goods immediately;
  - Customers using more than one (1) card to purchase the goods or services.

Chip card processing

A card which has a microchip embedded means the card contains security data and software which provides greater protection for you and the Bank against fraudulent or counterfeit activity.

There are only two (2) ways to process a chip card through your terminal:

- 'Paywave' and 'Paypass' / Contactless Transactions; and
- Dipping the card into the merchant terminal.

Protection of PIN Entry

Encourage the cardholder to cover the PIN pad when entering their PIN to prevent the possibility of sighting by a third party.

How to safeguarding against skimming

EFTPOS skimming occurs when a customer's card and/or PIN data is illegally copied with the intent to create counterfeit cards or use compromised card data to conduct unauthorised transactions.

Criminals will look to either compromise your EFTPOS terminal or replace your EFTPOS terminal with a similar looking terminal they have already compromised.

The following checks should routinely occur to assist identify if your terminal has been compromised:

- Ensure the Merchant ID (MID), Terminal ID (TID) and trading name on the receipt has not changed;
- Confirm that the make, model and serial number (located on the back of the terminal) of the EFTPOS terminal has not changed;
- Confirm the terminal location hasn't changed;
- Confirm the condition of the terminal has not changed:
  - Is not damaged or appears to have been tampered with;
  - Cables are not missing or additional cables added; and
  - Increase or decrease in number of stickers on terminal or the colour of the terminal is slightly different.
- Ensure the area surrounding the EFTPOS terminal is clear to reduce the ability to hide cameras.

NB: Verifone is BOQ's 3rd Party Terminal Provider. There is a set process in place regarding a Verifone technician visit to your site. Verifone technicians will always:

- Make contact prior to their visit, and should never attend your site unannounced;
- Ask for the nominated contact when arriving at the merchant site; and
- Show their identification immediately on arrival at your site.

If you believe your terminal may have been compromised or are suspicious of receiving fraudulent / counterfeit information please contact the Merchant Help Desk on 1800 700 226 and select option 3.

Chargeback

What is a chargeback?

'Chargeback' is a term used when a card transaction is reversed and your nominated settlement account is debited with the amount of the sale.

Generally, if a cardholder disputes a transaction and you don't have sufficient evidence to show that the cardholder authorised the transaction, then you will be liable for the chargeback. For this reason, it is important that your business keeps good records to enable adequate investigation of any card transaction dispute and to assist with reduction of the risk of unnecessary chargebacks occurring.

The most common reasons for chargebacks include:

- Customer disputes;
- Fraud; and
- Processing errors by either the merchant or their Bank.

Chargeback timeframes

Chargebacks can take place up to 180 days from the date of the transaction being disputed.

What are the most common chargebacks?

Transaction not recognised by cardholder

Definition: The cardholder (merchant's customer) contacted their Bank (Issuer Bank) to lodge a dispute stating that they did not recognise a particular transaction appearing on their card statement. This means they do not recognise the merchant's name and/or location.

The 'retrieval request' (dispute) did not resolve the issue. The cardholder's bank creates and processes the chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale).

Hints on how to minimise this type of chargeback

Where possible always respond to a 'retrieval request' with the required documentation. This will automatically reduce the number of chargebacks where the cardholder does not recognise the merchant's name and / or location; and

- The merchant's name is the single most important factor in the cardholder's recognition of the transaction appearing on their card statement. Therefore it is critical that the merchant name, while reflecting the merchant's 'Doing Business As' name, also be clearly identifiable to the cardholder. The merchant will need to supply more information around their merchandise, location and items the cardholder purchased.

Goods / Services not provided by Merchant

Definition: The cardholder (merchant's customer) contacts their Bank (Issuer) to lodge a dispute advising merchandise / service had not arrived from the merchant by the expected delivery date.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated settlement account is debited with the amount of the sale).

Hints on how to minimise this type of chargeback

Goods / Services delivered:

- Send to BOQ evidence of the delivery, such as a delivery receipt signed by the cardholder or a carrier's confirmation that the merchandise was delivered to the correct address

Delivery date has not expired:

- Send a copy of the transaction receipt to BOQ pointing out that the delivery date has not yet expired

Delayed delivery of merchandise:

- If the delivery of the merchandise is to be delayed, notify the customer of the delay and the expected delivery date. As a service to your customer, provide the customer the option of proceeding with the transaction or cancelling it. Send copies of this correspondence to BOQ for assessment.

Cardholder did not authorise – card not present (Mail Order / Telephone Order - MOTO) transaction

Definition: The cardholder (merchant's customer) contacted their Bank (Issuer Bank) to advise they did not authorise a 'card not present' (MOTO) transaction appearing on their card statement. There could be several reasons for not recognising the transaction:

- Cardholder did not recognise the merchant's name as it is different to the shop name; or
- Cardholder did not authorise or participate in the transaction.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale).

NB: An authorisation obtained on a fraudulent / counterfeit card only confirms that the funds were available at the time of the transaction. This authorisation does not confirm that the cardholder is the one making the transaction and therefore can result in a chargeback to the merchant, and at times, the loss of either goods or services.

Hints on how to minimise this type of chargeback

Cardholder did not recognise the merchant's name:

- The merchant's name is the single most important factor in the cardholder's recognition of the transaction appearing on their card statement. Therefore it is critical that the merchant name, while reflecting the merchant's 'Doing Business As' name, also be clearly identifiable to the cardholder. The merchant will need to supply more information around their merchandise, location and items the cardholder purchased.

Cardholder did not authorise or participate in the transaction – fraudulent / counterfeit transaction:

- Where possible the merchant should obtain the CVV2 from the cardholder (the 3 digit security number on the back of the card) – this helps validate that the customer is in possession of the card at the time of an order (it still however, might not mean the genuine cardholder is the one making the purchase);
- Be aware of urgent requests for quick or overnight delivery from the customer, as it can be a sign for possible fraud;
- Be aware of customers who are ordering above your usual transaction size and don't care about additional costs that may be involved;
- Customer has asked for goods to be delivered to a Post Office box.

Credit not processed by merchant

Definition: The cardholder (merchant's customer) contacts their Bank (Issuer Bank) acknowledging participation in a transaction for which goods were returned or services cancelled, but the credit has not appeared on their card statement.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale)

Hints on how to minimise this type of chargeback

- Always refund a sale value to the same card that the transaction was originally processed on, and retain evidence of the refund processed.
- Never process a refund, direct to a Bank account, by cash or by other means.

Cancelled Recurring Transaction

Definition: The cardholder (merchant's customer) contacts their Bank (Issuer Bank) to notify that they have cancelled a recurring transaction however it is still appearing on their card statement.

The 'retrieval request' (dispute) did not resolve the issue and therefore the cardholder's bank creates a chargeback to the merchant via BOQ (i.e. the card transaction is reversed and your nominated account is debited with the amount of the sale).

Hints on how to minimise this type of chargeback

- Always process the cancellation in a timely manner.
- Send notification to the cardholder advising the cancellation request has been processed.

Fraud/Counterfeit Cards/Skimming

What is a fraudulent transaction?

A fraudulent transaction occurs when a card account is used through the theft of the account holder's card number and card details. This can occur in several ways:

- Stolen / lost card; and
- Counterfeit cards (mainly created via skimming).

NB: An authorisation obtained on a fraudulent / counterfeit card only confirms that the funds were available at the time of the transaction. This authorisation does not confirm that the cardholder is the one making the transaction and therefore can result in a chargeback to the merchant, and at times, the loss of either goods or services.

Hints on how to minimise fraudulent transaction

- Where possible for all MOTO transactions obtain the CVV2 3 digit number
- Recognise suspicious orders, such as:
  - Transaction requests that are above your average purchase value;
  - Delivering to overseas addresses;
  - Customers who do not care what the value of the purchase is or additional costs (such as shipping / postage);
  - Delivery to post office boxes;
  - Rushed request where the cardholder advises they needed to goods immediately;
  - Customers using more than one (1) card to purchase the goods or services.

Chip card processing

A card which has a microchip embedded means the card contains security data and software which provides greater protection for you and the Bank against fraudulent or counterfeit activity.

There are only two (2) ways to process a chip card through your terminal:

- 'Paywave' and 'Paypass' / Contactless Transactions; and
- Dipping the card into the merchant terminal.

Protection of PIN Entry

Encourage the cardholder to cover the PIN pad when entering their PIN to prevent the possibility of sighting by a third party.

How to safeguarding against skimming

EFTPOS skimming occurs when a customer's card and/or PIN data is illegally copied with the intent to create counterfeit cards or use compromised card data to conduct unauthorised transactions.

Criminals will look to either compromise your EFTPOS terminal or replace your EFTPOS terminal with a similar looking terminal they have already compromised.

The following checks should routinely occur to assist identify if your terminal has been compromised:

- Ensure the Merchant ID (MID), Terminal ID (TID) and trading name on the receipt has not changed;
- Confirm that the make, model and serial number (located on the back of the terminal) of the EFTPOS terminal has not changed;
- Confirm the terminal location hasn't changed;
- Confirm the condition of the terminal has not changed:
  - Is not damaged or appears to have been tampered with;
  - Cables are not missing or additional cables added; and
  - Increase or decrease in number of stickers on terminal or the colour of the terminal is slightly different.
- Ensure the area surrounding the EFTPOS terminal is clear to reduce the ability to hide cameras.

NB: Verifone is BOQ's 3rd Party Terminal Provider. There is a set process in place regarding a Verifone technician visit to your site. Verifone technicians will always:

- Make contact prior to their visit, and should never attend your site unannounced;
- Ask for the nominated contact when arriving at the merchant site; and
- Show their identification immediately on arrival at your site.

If you believe your terminal may have been compromised or are suspicious of receiving fraudulent / counterfeit information please contact the Merchant Help Desk on 1800 700 226 and select option 3.

PCI-DSS-Protection Cardholder Information

The following guidelines will assist in minimising the risk of cardholder data being compromised, as well as assisting to protect your business against potential liability and costs associated with investigations:

- Always store all cardholder information in a secure environment only accessible by authorised employees / personnel;
- After required timeframe (12 months) destroy all cardholder information resulting in unreadable documents, e.g. shredding;
- Never accept or store any cardholder information via email;
- Never swipe or insert a card through a device other than your EFTPOS terminal which has been approved and installed by BOQ;
- Never sell, buy or exchange any cardholder information other than to BOQ or when legally requested; and
- Never ask for or retain under any circumstance any cardholder's PIN data.

Websites

BOQ suggests for further information you visit the below websites:

- www.apca.com.au
- www.pcisecuritystandards.org
- www.visa.com.au
- www.mastercard.com.au/merchant

Contact Information

For more information please refer to your Merchant Agreement or contact the BOQ Merchant Helpdesk on 1800 700 226 and select option 3.

You can also visit
www.boq.com.au/merchant