Fraud Education

Fraud Education

Protecting your Pago Merchant Facility

Fraud can happen to any business that accepts debit and credit card payments and can have a significant financial and reputational impact on your business.

Here's some information to help protect your business and limit the impact of fraud.

1. How risky is the way you do business?

The way your business processes and accepts a transaction can carry a higher level of risk than others.

Examples of Lower Risk Transaction Processing

- Face to face, in store purchases
- Transactions where the card is tapped or inserted into the Pago terminal
- The types of products and services you offer can also increase your risk because fraudsters will often target high value goods with easy resale potential. Examples of these goods include electronics, furniture, jewellery and luxury goods etc

Examples of Higher Risk Transaction Processing (not limited to)

- First time customers
- International customers
- Card not present transactions – Mail order/Telephone order, Internet, IVR authorisation and settlement
- Manually keyed transactions
- Pre-payment and deposit taking

2. Help keep your business safe

You can do this by implementing the below;

- Train your employees on how to verify cardholders and look out for suspicious transactions
- Develop and regularly refresh all employees on transaction handling processes and procedures as per the user guides issued with your merchant facility
- Create a daily checklist of terminal tampering checks that must be completed daily before opening for business
- Develop and maintain a secure customer data base to track buying patterns, addresses and customer behaviours
- Create an 'approval and order fulfilment' process for new employees and new customers requesting high value orders

If accepting MOTO, here's some things to look out for some helpful hints;

- Be mindful and vigilant when an unusual or high-value MOTO request is made
- Any unusual requests from the cardholder regarding the collection or delivery of the order, such as agreeing to pay for relevant freight or postage costs when it isn't usual practice.
- Be cautious of international cards being utilised for domestic use.
- If the products are being delivered, you can request the cardholder to show a Photo

(a) ID, and the original card used for the transaction to confirm the identity matches the
(b) name on the physical card.

3. Eftpos fraud prevention

When taking a payment in store, there are a few steps you and your employees should take to ensure the card and owner are genuine, and that your EFTPOS terminal is secure.

Never accept a card if:

- The terminal doesn't recognise the card
- The card expiry date has passed
- The card or the signature has been visibly altered or tampered with
- The signature doesn't match that on the back of the card
- The card is damaged

If any of these occur, ask the cardholder for another form of payment. This applies to all card types

You should also:

- Never hand key transactions if the card is present at the time of transaction
- Never give the terminal to the cardholder to enter the card details
- If the terminal response is 'declined', ask for an alternate form of payment
- Be wary if a customer presents a card that rejects and then switches to another card

We also recommend these steps:

- Closely monitor all refunds to ensure they have a legitimate corresponding sale
- Establish processes for only a small group of staff to process high value refunds
- Be alert to changes in staff behaviour or a sudden increase in their spending habits or wealth
- Never refund a card transaction if:
  The customer asks you to refund the transaction in cash, to a bank account, through Western Union or different card. Credit cards can accept refunds even if the card is reported as lost or stolen

4. Chargebacks

A chargeback is a reversal of a credit card payment that occurs when a cardholder disputes a transaction they didn't authorise. This means you don't get paid for the goods and services relating to the transaction, even if you've already provided them. You may also have to pay fees for the chargeback to be investigated and processed.

A cardholder has up to 18 months to dispute a transaction from the transaction date. Alternatively, the cardholder has up to 120 calendar days to dispute a transaction should the business have not delivered the goods and/or services that should have been provided.

The most common Chargebacks reasons are:

- Card wasn't valid at the time of the transaction
- Goods and Services purchases were not received
- The transaction has been duplicated
- The merchants promised a credit that has not been processed
- The goods and services purchased were not as described or defective
- The incorrect amount was charged

4.1 **How the chargeback process works:**

- A dispute is raised against you, the merchant, by the cardholder or the cardholder's bank
- We receive notification of the dispute and will notify you via email. In the event of a fraudulent chargeback, we may debit your account immediately.
- You may disagree with the dispute. If so, you may be asked to provide supporting evidence depending on the dispute reason. Instructions will be provided within the email
- If the cardholder dispute is resolved in the merchant's favour, the chargeback request is returned to the cardholder's bank and the cardholder must pay their statement
- If the cardholder dispute is not satisfactorily resolved or supporting evidence not provided within the required timeframe, the chargeback will remain in place

5. Protecting your EFTPOS terminal

It's important to keep your terminal secure to ensure it cannot be tampered with or stolen.
Here are some tips on how to protect your EFTPOS terminals:

- Keep the terminal in a secure location
- Never leave your terminal unattended
- Create end of day checks to ensure all terminals are accounted for and in working order
- Ensure all employees are fully trained
- Best practice would be to not disclose your terminal password to anyone. However if you need to tell other staff members, make sure you only disclose to a small group of staff to process refunds.
- Avoid having security cameras at locations which can capture you entering passwords and customer card details.

There may be times when our field technicians need to work on the terminal e.g. to inspect or replace it. Make sure they have an appointment and provide ID, and if you suspicious or have any questions call us on 1800 xxx xxx.

If you believe your terminal, or any other equipment associated with your facility is stolen or tampered with, call us immediately on 1800 xxx xxx.

6. Protect your customers data

To protect your business and cardholders from fraud, you need to be aware of how you manage your customers' information.

Always:

- Ensure that any card information you store or transmit across the internet/other networks is encrypted and compliant in accordance with the Payment Card Industry Data Security Standard (PCI DSS)
- Ensure that information you store is only accessible to people who are authorised to manage or view that data
- Store any records containing information, such as copies of offline paper vouchers, in a secure place only accessible by authorised people
- If you need to dispose of card or customer data, ensure it is unreadable and all documents shredded

- If you use another business partner, other than the Bank, to help you manage cardholder data, make sure they are PCI DSS compliant.

Never:

- Disclose or share any card information without a justifiable business reason
- Request, use or store a card number for any purpose that is not related to a transaction
- Process a card through any card reading device not authorised by us
- Ask for a cardholder's PIN
- Store or collect a cardholder's CVV/CVC