How to combat card fraud

A guide to detecting and preventing card fraud.

SUNCORP BANK
Business

Contents

Introduction.

In the vast majority of cases, card transactions are a safe and convenient way to do business. However, merchants have always faced some risks when accepting card transactions and those risks have increased and become more complex as technology advances at lightning speed. Hi-tech crime is a major challenge, but Suncorp Bank can help you minimise your losses.

Suncorp Bank has prepared this guide to give you a range of precautions and advice you can take to minimise these risks and continue to trade confidently and prosperously.

Card fraud falls into two broad categories:

1. **Card Present fraud**. This occurs face-to-face with the offender physically transacting with an illegitimate card. Illegitimate in this context means not authorized by the cardholder.
2. **Card Not Present fraud**. This type of fraud is related to internet purchases or mail order or telephone order (MOTO).

In both forms of card fraud, the items listed below are targetted by fraudsters because of their high value and/or ease of resale. If you trade in any of these items, be aware that you may be at higher risk of card fraud:

- Computers, laptops and tablets
- Electrical appliances
- Jewellery
- Furniture
- Goods which are easily disposed of for cash e.g. cigarettes, alcohol and gift cards.

Card Present fraud.

While Card Present (face-to-face) fraud carries less risk than trading in a Card Not Present environment, there are still significant dangers. Below is a list of suspicious indicators. Beware of customers who:

- Appear anxious, nervous or impatient
- Try to rush or distract you while you're processing the transaction
- Make unusually large orders
- Arrive on closing time
- Make repeat purchases in a short period of time
- Split transactions i.e. Offer more than one card for a single purchase
- Purchase multiple numbers of the same item with no interest in size, colour, style or price
- Purchase large items, but reject home delivery even when it's included in the purchase price. Perhaps they don't want the merchant to know their address
- Make a large purchase on a newly valid card. You can determine whether the card is "newly valid" by having a look at the "Valid From" date on the front of the card. Sometimes cards are stolen while being mailed from the bank to the rightful cardholder.

How to reduce the risks of Card Present fraud.

Merchants should also take the following precautions:

- Inspect the card closely, checking that the "valid from" and "valid through" dates include the current date
- Check the card has the appropriate security features
- Closely inspect the card to determine whether it's been tampered with

- Visa cards only - Ensure the first four digits of the embossed card number match the four digits printed immediately above or below the embossed number
- Check that the abbreviated card number on the sales receipt matches the corresponding digits on the card. If the digits don't match, this is a clear indication the card is counterfeit
- Tilt the card to check the hologram on Visa and MasterCard cards move and/or change colour
- Always insert or tap the card through your terminal.

Card Not Present fraud.

As you would expect, Card Not Present fraud is more common than Card Present fraud. Fraudsters prefer to make Card Not Present purchases due to the anonymity. Because Card Not Present fraudsters operate via internet or mail order and telephone order (MOTO) transactions, it means they can commit their crimes all over the world.

Below is a list of some red flags that you should consider when accepting Card Not Present transactions. Remember that one of the flags alone should attract attention while more than one should raise alarm bells:

- The order is unusually and inexplicably large
- The order is for goods that you do not normally deal in
- The order is for multiple quantities of the same item
- The customer places a number of orders within a short space of time
- The customer places the order using multiple cards
- When the order is placed and the first card offered is declined, a second card is immediately produced. This suggests they may have quick access to numerous, possibly stolen cards
- The order requests express freight
- The order is shipped to a country where the goods could easily be purchased locally. Why would the purchaser pay shipping expenses and wait longer for the goods to arrive?
- The order requests delivery to a post office box
- The order requests the goods be shipped to a third party
- The purchaser pays for an item with a card by phone but collects the goods from the store. This allows them to make purchases without supplying personal information

- You receive multiple orders within a short period of time on card numbers that are very similar, such as where only the last four digits differ
- Goods or services are ordered then cancelled with a request to refund the funds in ways other than refunding the card that was used for the purchase.

A red flag for fraud.

Your fraud risk increases with any overseas order. All overseas orders should be checked, especially if they're from a country you don't usually receive orders.

However, some countries pose a bigger risk. Transactions originating from the following countries are proven to have a disproportionate level of card fraud:

- Ghana, Nigeria, Ivory Coast (and West Africa in general)
- Indonesia
- Singapore
- Countries in Eastern Europe.

How to reduce the risks of Card Not Present fraud.

Merchants can minimise fraudulent purchases from Internet and MOTO transactions by taking these steps:

- Ask the purchaser to provide the CVV2 (Visa) or CVC2 (MasterCard) three digit number located on the signature panel of the card
- Never send goods to a post office box
- Beware of split purchases. Multiple cards being used for a single purchase are highly suspicious and not permitted under our Terms and Conditions
- Request that the purchaser provides a fax, or scanned and emailed copy of their driver's license
- Ensure that the customer's billing and delivery addresses are consistent

- Verify addresses and phone numbers provided (an online White Pages search should do the job)
- Obtain a signed receipt from the cardholder when the goods are delivered
- When a large number of different goods are ordered, telephone the cardholder to confirm the order. Quite often fraudsters don't keep records and therefore can't confirm details
- Beware of customers that are unable to talk to you over the phone
- Never refund in any other manner than to the card the purchase was made on.

Don't continue to attempt authorisation if you receive a decline.

Payment card industry data security standards – Your guide to protecting cardholder data.

Your customers' data is your responsibility.

Data theft is a growing global concern. It's your responsibility to safeguard your customers' details whether you store the data yourself or use a third party data storage company.

To help you ensure the security of highly sensitive personal financial information, Suncorp Bank has developed the booklet "Payment Card Industry Data Security Standards - Your guide to protecting cardholder data".

Visit www.suncorpbank.com.au/PCIDSS to view the guide.

A Merchant's website responsibilities.

You need to ensure when developing your website you consider the following:

- That it offers an accurate description of the goods and services you're selling
- That it contains clear explanation of shipping practices and delivery policy/timeframe
- That card logos are displayed wherever payment options appear
- That the refund/return policy is clearly displayed and explained and complies with the relevant consumer law
- That it displays total cost of the goods or services purchased (including shipping charges)
- That it contains all required contact details – trading name, address and Australian Business Number (where applicable)
- That it only processes Australian dollar amounts and settles into Australian dollar accounts
- That the URL and trading name are not significantly different, thus avoiding cardholder confusion
- That it contains the security capabilities and policy for transmitting of payment card details
- That export restrictions are clearly outlined
- That your consumer data privacy policy is explained clearly i.e. – what you do with any customer information you collect
- That each merchant's domain name has individual payment pages. It must not link to another website where payment is made for the goods or services offered on the originating site.

When developing your website, you need to ensure your website does not:

- Sell illegal goods or encourages violation of export controls, obscenity or gambling laws. This applies to both Australian laws and regulations and those of any other jurisdiction you're providing you goods and services to
- Contain pornographic material
- Offer for sale goods or services that may be considered obscene, offensive or dangerous
- Use unaccredited payment pages
- Use digital certificates to establish a secure browser session
- Offer for sale goods or services that do not reflect the nature of goods or services for which the merchant facility was approved.

Is that transaction authorised?

Ensuring that you are dealing with an authorised card is fundamental. Please take the time to understand exactly what the term ‘authorisation’ means. It could save your business from serious financial losses.

A transaction is authorised if:

- The card number is valid
- It holds sufficient funds available to cover the transaction
- The card hasn’t been reported lost or stolen (though it may actually be stolen or compromised and the rightful owner is unaware of the breach).

Beware what ‘authorisation’ doesn’t mean:

- There’s always the risk that the customer has somehow illicitly obtained the card number without being in possession of the card. That’s why authorisation does not confirm that the person providing the card number is the legitimate cardholder
- Please be aware that obtaining an authorisation for each transaction doesn’t guard you against fraud or chargeback.

Laundering leaves your business exposed.

Laundering is a serious breach of Suncorp Bank policy and exposes your business to major financial loss.

Put simply, laundering involves a credible merchant processing transactions on behalf of another merchant. Automatically the red flag must go up as to why this third party would want a credible merchant to take part in this kind of activity. Experience tells us that laundering happens because a disreputable operator doesn't have access to card facilities because of an unscrupulous past.

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

Ensure that your EFTPOS Terminal is secure.

Suncorp Bank provides our merchants with the very latest information on EFTPOS terminal and cardholder data security. Protecting your customer's data is a priority.

To help merchants protect their terminals and customer information, we've prepared the following list of suggestions:

- Always update your software to the latest version as soon as it's available
- Check regularly to make sure your EFTPOS terminal(s) hasn't been tampered with
- Lock your terminal(s) away when the store is closed
- Check that any nearby CCTV cameras aren't directed on cardholders entering details at your EFTPOS terminal(s)
- Always supervise your terminal(s) during operating hours
- Only allow authorised and fully trained staff to use your EFTPOS terminal(s)
- Only allow authorised Suncorp personnel, with correct identification, to perform maintenance on your terminal
- Never allow maintenance to be carried out on your EFTPOS terminal without prior notice from Suncorp Bank
- There should never be additional cables running from your EFTPOS terminal
- Secure and change regularly your Merchant (refund) password

Notify Suncorp Bank Merchant Services (24 hours / 7 days a week) on 1800 836 055 immediately if:

- The EFTPOS terminal goes missing, is damaged or has been interfered with
- The EFTPOS terminal is printing incorrect receipts and other data
- Attempts are made to either exchange or remove your EFTPOS terminal, or carry out maintenance, without prior notification from Suncorp Bank
- Unauthorised personnel attempt to carry out maintenance on, or remove, your EFTPOS terminal without appropriate security identification.

More information on terminal and data security is available at www.suncorpbank.com.au/PCIDSS

Suncorp Bank is here to help keep you safe from card fraud.

At Suncorp Bank, we're committed to helping our merchants protect their business, and their customers, from card fraud.

If you have any questions regarding card security, or you suspect your business may have experienced card fraud, contact us today.

suncorpbank.com.au

13 11 75

local branch

SUNCORP BANK Business