Card Payment Fraud Minimisation Guide
ANZ Merchant Business Solutions

INTRODUCTION

Fraud is a risk for any business that accepts cards. It can occur at any time and have a significant financial impact on your business. At ANZ, we assist our customers to minimise the likelihood of fraud occurring in their business through on-going education. The more you know about the potential risks the more you will be able to protect your business.

If a debit or credit card transaction turns out to be fraudulent, it may be charged back to you and could end up costing you more than the original sale. High levels of fraud and chargeback can also attract penalties from the Card Schemes (Visa, MasterCard and UnionPay) and can result in the termination of your merchant facilities.

Please take the time to read and familiarise yourself with this guide. It provides information to assist you in indentifying and minimising fraud and chargebacks occurring in your business.

For further information, please refer to your Merchant Operating Guide and the Merchant Agreement Terms and Conditions or if you wish to speak with someone about your merchant facility or this guide, please contact our Merchant Business Team on **0800 473 453**.

PROTECTING YOUR BUSINESS

Some types of card transactions carry a higher level of risk than others. The products you sell can also increase your risk as fraudsters often target businesses selling higher value goods with easy resale potential.

Higher Risk transactions may include:

- First time customers
- International orders
- Card not present transactions, including email, internet, mail and phone orders
- Any transaction where the card is not swiped, inserted or tapped on an EFTPOS terminal
- Transactions which are manually keyed into an EFTPOS terminal
- Manual transactions where no authorisation has been obtained.

Lower Risk transactions may include:

- Transactions where the card is swiped, inserted or tapped on an EFTPOS terminal
- Manual transactions where a signature and authorisation have been obtained
- Internet transactions authenticated by Verified by Visa or MasterCard SecureCode.

First Line of Defence

You and your staff are the first line of defence against fraudulent card transactions and you should always be on the lookout for any unusual behaviour or spending patterns.

For example – if a first time customer to your business is buying a large quantity of your goods and is not concerned about the price, colour, size, etc and their purchase is much larger than a normal purchase and it all seems too good to be true, it probably is. If you come across a situation like this, it is better to ask for an alternative form of payment, i.e. a bank deposit or cash.

WHAT ARE YOUR RESPONSIBILITIES?

Your responsibilities are outlined in your Merchant Agreement Term and Conditions, the Merchant Operating Guide and any applicable Additional Service Schedules (your Merchant Agreement). You must follow all the instructions in these documents.

It is your responsibility to verify that the purchaser of your goods and/or services is the genuine cardholder and to validate all cards presented.

You MUST:

- Accept all valid cards for payment
- Follow correct authorisation procedures and always follow terminal prompts
- Ensure the customer authorises all credit card transaction receipts (unless the transaction is by internet, phone, fax, mail order or contactless under NZD$200). Customers authorise credit card transactions by using a Personal Identification Number (PIN) or signing transaction receipts.
- Provide a copy of the authorised transaction receipt to the customer
- Be alert to possible card fraud and report all instances
- Protect account and transaction information at all times
- Notify us of any material change to your business. This includes, but is not limited to a change in business name or if you would like to change the types of goods and services your business sells
- Ensure the physical security of your merchant facility. Never leave your terminal unattended during trading hours or let a customer tell you how to process a transaction
- Always identify technicians attending your premises and never reveal any passwords. Fraudsters may approach your business posing as a terminal, electrical or phone technician wanting to access your terminal. They may then process refund transactions or insert card readers in to your terminal that will enable them to steal cardholder information whenever a card is swiped or inserted.

You MUST NOT:

- Give cash out with a credit card transaction
- Process transactions on behalf of another business through your merchant facility
- Transfer funds from a card in your name via the merchant facility to your settlement account.

If you fail to comply with any of the above responsibilities you are in breach of your Merchant Agreement with us and this may result in the termination of your merchant facilities and possible fines from the Card Schemes.

CARD PRESENT TRANSACTIONS

A card present transaction where the card and cardholder are present in person for the transaction is less risky than a card not present transaction, however fraud can still occur. You should always undertake the security checks described below for card present transactions to ensure the purchaser is the genuine cardholder and that the card is not a counterfeit or been tampered with.

Checks for Credit and Debit Cards

Most credit cards have the card details embossed on them

- Embossing should be even with all numbers the same size and shape
- Check the card expiry date is valid (UnionPay cards may not have an expiry date or display '00/00' – the EFTPOS Terminal will check whether the card is valid)
- Ensure the cardholder name is present and does not look like it has been tampered with
- Check the name on the card matches any other information provided.

Note: UnionPay Cards may be co-branded with another card scheme (e.g. Visa).

Check that there is a four digit number printed below the account number

- Even if scratched, this number can not be removed
- Check it matches the first four digits of the account number.

Note: Applicable to Visa only.

Card numbers

These start with a:

- '4' for Visa and have a total length of 16 digits
- '2' or '5' for MasterCard and have a total length of 16 digits
- '3', '4', '5', '6' or '9' for UnionPay and have a length between 13-19 digits.

Signature panel

- Card Security Code: There should be three additional numbers on the signature panel which must be present
- Check that the card has been signed and that the signature on the card matches the signature of the transaction receipt or any other signature provided.

Magnetic stripe

- Check the card has a magnetic stripe on the reverse.

Authorising Card Present Transactions

Authorisation for electronic debit and credit card transactions is online and automatic via a Personal Identification Number (PIN). A credit card transaction may also be authorised by signing the transaction receipt. Contactless Transactions under $200 can be authorised electronically without a PIN or signature (except internationally issued UnionPay Debit Cards).

If the transaction is authorised through an EFTPOS terminal, an 'accepted' or 'accepted with signature' message appears on the terminal and a transaction receipt prints.

If the card fails any validation checks or the transaction is declined:

- Request another form of payment or retain the goods
- If the 'declined' message tells you to keep the card, then do so if this can be done peacefully. Then phone the Contact Centre on **0800 269 296** for further instructions.

Additional Checks for Card Present Transactions

Take note of the customer's behaviour

During a transaction and while performing the card security checks, take note of the customer's behaviour. Individuals using credit cards fraudulently often behave unusually or appear overly anxious. The following behaviours can be used as a guide but do not necessarily indicate criminal activity. You should always let common sense be your guide.

Be alert for a customer who:

- Makes indiscriminate purchases without regard to size, colour or price
- Is unnecessarily talkative or delays a selection repeatedly until you are flustered
- Hurries you at closing time
- Requests you split the transaction over two or more cards
- Purchases an extended warranty without hesitation even though it may be costly
- Makes purchases, leaves the store, and returns to make additional purchases
- Pulls the credit card out of their pocket rather than a wallet
- Does not have a driver's license or another form of identification or says it is in the car
- Needs to see the card in order to sign a transaction receipt
- Chooses an item in store, requests delivery and says they will phone their credit card details through.

If you are suspicious of a customer and the card they are using:

No physical attempt should be made to prevent a cardholder from leaving. It is best to establish where the cardholder went to, and if using a motor vehicle, record the registration number and description of the vehicle. This information together with a full description of the cardholder and associates should be written down as soon as possible so it can be provided to the Police.

CARD NOT PRESENT TRANSACTIONS

Internet, mail and telephone order transactions are commonly referred to as card not present transactions. The cardholder and card are not present in person for these types of transactions.

If you are accepting card not present transactions, there is generally a greater risk of fraud. This is because fraudsters take advantage of the anonymity a card not present transaction provides. They are able to make purchases with or without a physical card, at anytime from anywhere in the world.

Obtain Additional Card Details

When taking an order for a card not present transaction as well as obtaining the standard information – credit card number, expiry date and full name – it is recommended you also retain the following additional information.

- IP Addresses
- Any customer location data
- 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.

Authorising Card Not Present Transactions

If you are processing transactions using an online payment gateway these are authorised electronically at the time of the transaction. If you are processing mail order or telephone order transactions using the IVR Authorisation and Settlement Service you must call the Credit Card Authorisation Centre on **0800 741 100** to process the transaction.

- If approval is given, record the authorisation number as detailed in your Merchant Operating Guide and dispatch the goods
- If the authorisation is declined ask the cardholder for another form of payment or retain the goods.

Note: Card Not Present Transactions using the IVR Authorisation and Settlement Service is not available for UnionPay transactions.

Delivery of Goods

- If a courier delivers the goods, ensure the courier company returns the delivery acknowledgment so the signature of the recipient can be verified
- Ensure goods are not left at vacant premises or left with a third party
- Confirm suspicious orders separately before shipping
- Do not send goods that are not part of your core business.

Suspicious Orders

Being vigilant about unusual spending patterns 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.

Be wary when:

- Recurring or sequential data elements appear. Look for transactions that might be 'testing' your system (e.g. multiple sales to the same address)
- Multiple cards are presented with multiple declines within a short period of time generally via your Internet payment page. These cards may have the same BIN (first six digits) or may appear to be sequential with only the last four digits changing
- You are requested to split transactions over a number of cards
- A customer places a number of orders within a short space of time
- Items that are ordered in unusual quantities and combinations and/or greatly exceed your average order value
- An order is requested to be delivered quickly. Fraudsters will often want their illegally obtained items as soon as possible for quick resale
- An order originates from Internet addresses using free email services, i.e. Yahoo, Hotmail, Gmail. They do not require a billing relationship or verification that a legitimate cardholder opened the account
- Orders are placed where the purchaser admits it is not their card being used
- Orders are being shipped to international destinations you may not normally deal with, especially third world countries
- Orders are received from locations where the goods or services would be readily available locally
- You receive orders for additional products you do not normally sell
- Orders are cancelled and refunds are requested via telegraphic transfer to an account other than the card used to make the purchase
- Goods or services have been ordered over the phone to be collected in person at a later date. When the cardholder collects the goods, ensure the following:
  - The credit card is presented at the point of collection. Check the name on the credit card is the same as the person name your recorded when the order was placed
  - Check the card security features
  - Ask the cardholder to sign an acknowledgement form to confirm they have received the goods
  - The signature is the same as that on the back of the card
  - Ask for suitable identification (photo ID preferable)
  - Be suspicious if a third party wants to collect goods on behalf of the cardholder.

International Orders

We suggest that you take extra care when receiving any international orders particularly large orders (much bigger than your average order size) and those originating from countries you do not normally deal with.

IF SUSPICIOUS – DO NOT FULFIL THE ORDER

If you are suspicious of the purchaser or the transaction and cannot verify that the payment details provided are genuine, ask for an alternative form of payment. If the customer is unable to provide an alternative payment, we recommend that you do not process the order.

Reducing the Risk of Card Not Present Transactions

You can help minimise the possibility of card not present transaction fraud by implementing the following measures:

- Develop a standard credit card transaction checklist that all staff must use when taking an order
- Develop and maintain a secure customer database to track buying patterns and identify changes in buying behaviour
- Discuss additional security with your service provider or an IT expert to help you redevelop your web/payment page. This could include blocking suspect IP addresses, BIN ranges and using Verified by Visa and MasterCard SecureCode.

If you think that your website has become a target for fraud, we suggest that you shut the site down for a short period of time and conduct an investigation on where the fraud is coming from. Once you have established the threat, block the IP address from which the orders are originating if this is possible.

Card Verification Value (CVV2/CVC2) or Card Identification Number (CID)

The Card Verification Value is the three-digit number located on the signature panel of the credit card.

If the purchaser cannot provide this number it is likely that they are not in possession of the card and they may be using card details that they have fraudulently obtained. It is important to note that validation of the CVV2 or CID is not a guarantee of payment or that the card is not a stolen card, it simply confirms that the purchaser has the card in their possession.

To prevent the Card Verification Value or CID data from being compromised or stolen never keep or store this data.

Note: UnionPay Debit Cards may not have a Card Verification Value or Card Identification Number.

Verified by Visa and MasterCard SecureCode

Verified by Visa and MasterCard SecureCode are online, real time security tools that can help protect your business against certain chargeback types.

When a cardholder makes a purchase on your website (if you are a participating business), the card number is recognised as being registered in the program and a Verified by Visa and MasterCard SecureCode window will appear. The cardholder will then be prompted to enter their verification which is then forwarded to their card issuer to verify the cardholder's identity and card number.

Following confirmation, the window disappears and the cardholder is returned to the checkout screen. If the cardholder is not confirmed, the transaction will be declined.

REFUND FRAUD

Refund fraud is a common type of fraud which involves issuing credits (refunds) via your EFTPOS terminal. It is often committed by employees processing refunds to their own card. To avoid detection they may create a large sale on a fraudulent card then process a refund to their own card. Refunds may also be processed to their own cards without a corresponding sale.

To guard against this type of fraud, we recommend you:

- Closely monitor all refunds, checking they all correspond to a legitimate sale and are refunded back to the card used in the original purchase
- Pay particular attention to large refund amounts or an increase in the number of refunds
- Restrict access to your refund card and/or refund PIN
- Watch for high volumes of 'key entered' transactions – key entered transactions are where the card number is entered into a terminal by hand instead of swiping or inserting the card
- Be alert to changes in staff behaviour or sudden evidence of an increase in their wealth
- Be wary of staff taking cash sales and balancing by processing fraudulent card transactions.

CHARGEBACKS

Chargebacks can have a financial impact on your business. A chargeback is the term used for debiting your bank account with the amount of a transaction that had previously been credited.

A chargeback occurs when a cardholder (or their bank) raises a dispute in connection with a card transaction. If the dispute is resolved in the favour of the cardholder, the transaction is 'charged back' to you and the value is debited from your settlement account. You are financially liable for all chargebacks that occur against your business.

There are a number of reasons why a transaction may be charged back. Some of the most common reasons are listed below. They can be broadly put into two categories, either where the cardholder is disputing the transaction, for example the card or cardholder was not present at the point of sale or they do not recognise the transaction on their statement and secondly, where you may have made an error processing the transaction.

Common Chargeback Reasons

- Processing errors
- Unauthorised use of a card
- Unauthorised transactions
- Invalid card account number
- Transaction exceeds floor limit
- Incorrect transaction amount
- Expired card
- Failing to respond to a retrieval request
- Pre-authorisations that are completed for higher amounts
- Merchandise not received by purchaser or wrong goods sent.

A cardholder or their bank can generally raise Chargebacks up to 120 days (or 180 days for UnionPay) from the transaction date or from the date the goods or services should have been provided. For this reason, you are required under your Merchant Agreement to retain all transaction receipts for a minimum of 18 months.

If a transaction is disputed, the bank that holds the account of the cardholder in question will notify us and we will notify you of the dispute. If our transaction records cannot show sufficient proof of the transaction, you will be notified in writing and asked to respond in writing by the due date on the notification with sufficient information to validate the transaction.

If you fail to respond by the due date on the notification, cannot provide sufficient proof of the transaction, or we find proof that you have breached your Merchant Agreement the chargeback may be upheld and your account will be debited.

If you are subject to an excessive number of chargebacks, we reserve the right to review your merchant facilities and your merchant facility could be terminated.

Avoiding Chargebacks

- Make every effort to abide by the guidelines and rules set out in this document and in the Merchant Operating Guide
- In card not present transactions, if a fraudster is intent on defrauding you, it is very difficult to protect yourself. It is up to you to decide the amount of checking and what processes you have in place to lessen the chance of fraud. Usually, any fraud will manifest itself in the form of a chargeback well after you have sent the goods.

Note: When prompted, a signature is mandatory on all UnionPay Card transaction receipts.

PROTECTING ACCOUNT AND TRANSACTION INFORMATION

If you accept card payments from your customers, or use a third party service provider to do this (i.e. an Online Payment Gateway provider) you are responsible for ensuring that your customer's payment details are kept secure at all times.

The Payment Card Industry Data Security Standard (PCI DSS) defines industry best practices for handling and protecting credit card details. All businesses that process, store or transmit credit card data must be compliant with the standard. It details what information needs to be protected and/or made secure and provides you with a framework to control the risks and keep credit card information in your possession safe and secure.

Benefits of your business

- Ensuring the security of cardholder data can lessen the likelihood of a data breach resulting from your business
- Helps to identify potential vulnerabilities in your business and may reduce the significant penalties and costs that result from a data breach should one occur.

Failure to take appropriate steps to protect your customer's payment card details means you risk both financial penalties and cancellation of your merchant facility in the event of a data compromise.

Our website contains comprehensive information on the Payment Card Industry Data Security Standard.

SECURING YOUR EFTPOS TERMINAL

All EFTPOS terminals are equipped with a number of in-built security features which are designed to help protect your customers' information. By implementing the recommendations below, you can help protect your business, your customers and your reputation from Credit Card fraud or misuse through your EFTPOS terminal.

- Always ensure that your EFTPOS terminals are secure and under supervision during operating hours (including any spare or replacement EFTPOS terminals you have).
- Ensure that only authorised employees have access to your EFTPOS terminals and they are fully trained on their use
- When closing your store always ensure that your EFTPOS terminals are securely locked and not exposed to unauthorised access
- Never allow your EFTPOS terminal to be maintained, swapped or removed without advance notice from your terminal provider. Be aware of unannounced service visits and only allow authorised personnel to maintain, swap or remove your EFTPOS terminal, and always ensure that security identification is provided
- Inspect your EFTPOS terminals on a regular basis – ensure that there are no additional cables running from your terminals and that the casing has not been tampered with
- Check your EFTPOS terminal is located where it should be each time you open your store or premises and is printing the correct details on receipts
- Make sure that any CCTV or other security cameras located near your EFTPOS terminals can not observe cardholders entering details.

Contact ANZ on 0800 473 453 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 your terminal provider 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 have been tampered with.