ANZ WORLDLINE
Payment Solutions

Fraud Minimisation, Data Security and Chargeback Guide

Merchant Operating Guide

Fraud Minimisation and Chargeback Guide

Fraud is a problem for many merchants and can have a substantial financial impact on your business. This is often due to a lack of awareness about how to reduce the risks of fraud and the processes involved when faced with a customer Chargeback.

If a credit card payment turns out to be fraudulent, it may be charged back to you, possibly leaving your business out of pocket more than the value of the original sale. High fraud and Chargeback levels can also put the future of your merchant facility in jeopardy and it can result in your Merchant Agreement being terminated and attract penalties from the Card Schemes (Visa and Mastercard).

This guide is aimed at providing information to assist you in identifying and minimising fraud and Chargebacks to protect your business.

Please take the time to read through this guide in full and familiarise yourself with the Fraud Minimisation and Chargeback procedures.

For more information, please refer to your Merchant Operating Guide (where applicable) and the General Conditions of your Merchant Agreement.

Who to call for assistance

Credit card authorisation centre - 1800 999 205 (24/7)

ANZ Worldline Payment Solutions - 1800 039 025 (24/7)

ANZ Worldline Payment Solutions Merchant Fraud and Risk team - 1300 124 486 (8am - 5pm EST Monday-Friday)

Contents

1. Tips to Safeguard Against Fraud

Some credit card transactions present a greater risk to your business, depending on the method in which the card is processed – Card Present or Card Not Present (Mail, Telephone or Online Orders).

HIGHER RISK TRANSACTIONS MAY INCLUDE:

- Card Not Present transactions, including email, Internet and phone orders
- International orders (in particular, Africa & South East Asia)
- First time customers
- Any transaction where the card is not swiped through 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 (Card Present)
- Manual transactions where a card imprint, signature and authorisation have been obtained
- Internet transactions authenticated be Verified by Visa or Mastercard SecureCode.

2. Card Present Credit Card Fraud

Use the following guide as a checklist to help you protect your business from fraudulent credit card transactions via your merchant facility.

BEFORE YOU COMMENCE A TRANSACTION

Check:

- That it is a card you are authorised to accept
- To see if the card appears 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 3-dimensional
- In regards to the embossing:
  - the embossing should not be flattened (unless it is an unembossed card)
  - the embossing should be clear and even
  - the first four digits of the embossed number must match the pre-printed four digits on the card.

Check the signature during the transaction

- The card should be signed on the signature panel
- The signature or signature panel should not appear to have been altered
- The customer's signature on the Transaction Voucher should match the signature on the card if a PIN is not used.

When the transaction has been processed, check:

- The card number details against those printed on the Transaction Voucher
- The trading name and address details are correct
- That an approval number or approval code is printed on the Transaction Voucher.

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 (see Split Ticket Transactions)
- Ask for transactions to be manually entered
- Sign the Voucher or Transaction Voucher slowly or unnaturally.

To further safeguard against fraud

- Do not let anyone service or remove your terminal without strict instruction from ANZ Worldline Payment Solutions and first providing proper identification
- Do not allow equipment to be used by unauthorised persons
- Keep Merchant Cards secure from unauthorised staff and customers
- Make sure the black carbon sheets are destroyed if you make a manual imprint of the card
- Always follow the instructions contained in the "Processing a Refund" section of your Terminal Guide when processing a refund
- Store terminals and equipment in a secure environment and do not divulge Cardholder information (e.g. card numbers)
- Ensure you keep all merchant copies of sales vouchers in the case a dispute has been lodged against your business
- Advertise that your business will prosecute identified fraudulent activity on your website. This may help in deterring fraud. Make sure your anti fraud policy is displayed on your website.

3. Chip Card Processing

Chip Cards are Mastercard® and Visa (credit and debit) cards that are embedded with a security microchip that provides further protection to assist in decreasing 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**.

What to do if you are 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 Manual Transaction Voucher or the printed Transaction Voucher.

Remember:

- 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)

Remember: Your safety comes first – Do not take any chances.

4. Card-Not-Present Credit Card Fraud

Mail, Telephone and Internet Orders

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. Remember an order that seems too good to be true usually is - it's fraud.

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

Important:

"Authorisation" of a transaction involving a mail, telephone or Internet order is not a representation or warranty that the purchase is made by the Cardholder, or that the transaction will not be disputed for any reason. Under your Merchant Agreement, you may still be liable for and incur Chargebacks with respect to authorised transactions that are subsequently disputed by the Cardholder.

Chargeback Liability

A Cardholder can raise a Dispute/Chargeback with their bank (issuing bank) up to 120 days (dependant on the reason code) of the date of the transaction. The Cardholder can raise a dispute for many reasons, however, the most common reasons are Card Not Present Fraud, Transaction Not Recognised, Card Present Fraud, Duplicate Processing and Transaction Not Authorised (this is usually raised by the issuing bank, not the Cardholder). Cardholders may also raise a Dispute/Chargeback if goods are not received, are damaged, or are not as described.

Security Codes (CVC2, CVV2)

A Security Code, otherwise known as a Card Verification Code (CVC2) or Card Validation Value (CVV2), is a security feature designed to improve cardholder verification and help protect merchants against fraudulent transactions.

The Security Code is commonly captured for transactions where the cardholder is not present, for instance via a mail, telephone or eCommerce transaction and represents the last 3 digits on the signature panel on the back of the card.

Merchants using ANZ EFTPOS terminals can activate this security feature by contacting ANZ Worldline Payment Solutions on 1800 039 025.

As of 1 April 2012, all online payment facilities must also have the security code/CVV2 field enabled on their web payment page. Please refer to your Merchant Operating Guide for further mail order or telephone order processing instructions.

Common indicators of Fraud

- **Payments to a 3rd Party:** When your customer requests a payment be made to a 3rd party from the card payment to you, usually by Western Union Transfer. This may be disguised as a freight or logistics cost
- **High Risk locations:** Extreme caution should be used when sending goods to, or dealing with customers in the following locations which are generally considered to be high risk; Ghana, Nigeria, Ivory Coast (Western Africa in general), as well as Indonesia and Singapore
- **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, g-mail) 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. Also delivery to Post Office Boxes can 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:** 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:** Lack of details provided. 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. This allows them to make the purchase whilst providing no personal information (i.e; shipping, billing address), and the same card-not-present risks apply.

Obtain additional card details when taking an order as well as obtaining the standard information – credit card number, expiry date and full name – it is recommended you also obtain the following additional cardholder information:

- 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.

Best Practice Advice

- Capture the cardholder's Security Code/CVV2 or CVC2 represented by the last 3 digits on the back of the card

CVV2 - last 3 digits on the signature panel

- Call customer for follow up after the transaction. This will establish the contact details they have provided are valid
- Perform a web search using their company email address to help establish if the company is legitimate
- Verify customer's details in White Pages online. This can help identify if the customer's name and address match and are publicly listed
- Establish your own database to store details such as names, addresses, phone numbers, email & IP Addresses that have been used in known fraud transactions. Also keep a database of particular locations, such as suburbs and street names, which attract a high rate of fraud
- Never make a payment to a third party from the proceeds of a credit card payment that you have processed
- When processing a refund, always follow the instructions contained in the "Processing a Refund" section of your Terminal Guide
- Never process transactions for another business or friend where the transactions do not relate to your own core business
- Develop a standard credit card transaction checklist that all staff must use when taking an order
- Seek help: If you trade via the internet and use a 3rd party Gateway provider (Bureau), contact them for more fraud prevention measures
- If a courier delivers the goods, ensure the courier company returns the signed delivery acknowledgment. Ensure goods are not left at vacant premises or left with a third party
- Always use Registered Post if delivery by mail
- Obtain a manual imprint of the card and signature on delivery of the goods where possible
- Obtain an authorisation for all manual transactions
- Do not send goods that are not part of your core business.

Please contact ANZ Worldline Payment Solutions on 1800 039 025 and request to speak to the fraud team if you are concerned about a particular order.

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.

5. 3D Secure - Online Authentication Tool

Verified by Visa and MasterCard® SecureCode™

'Verified by Visa' and 'Mastercard SecureCode' are online, real-time Security tools that protects merchants against certain Chargeback cases, who trade online to validate that a Cardholder is the owner of a specific card number. Each Cardholder creates a unique password at the time of registration. When a Cardholder makes a purchase via the website of a participating merchant, the merchant's server recognises the Visa or Mastercard number and a Verified by Visa or Mastercard SecureCode window will appear.

The Cardholder will then be prompted to enter their password. The password is forwarded to the Cardholder's card issuer to confirm the Cardholder's identity and the 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.

Participating merchants are protected by their merchant bank from receiving certain fraud-related Chargebacks.

For further information about Verified by Visa and Mastercard SecureCode, please contact ANZ Worldline Payment Solutions on 1800 039 025.

Note: If you are operating via a 3rd party online Payment Service Provider (PSP), it is your responsibility to ensure that the correct risk management rules are applied to your payment facility. Please call ANZ Worldline Payment Solutions to ensure that your 3rd party PSP supports 3D Secure via ANZ Worldline Payment Solutions.

Internet and Mail Order & Telephone Order Sales

To ensure the customer's card details remain confidential, you must provide an appropriate envelope or instruct your customers to place their order coupons/application forms in sealed envelopes.

If ANZ Worldline Payment Solutions has agreed that you can accept cards as payment for mail, telephone and/or Internet orders, you may process requests for goods or services from Cardholders and charge the value to their credit card account.

Charges for the goods and services may be spread over specified periods as long as at all times you hold a current signed authority from the Cardholder.

Please note that there can be considerable risks involved with the processing of mail, telephone and Internet Transactions. Disputes may occur because appropriate card security checks and validation of authorities either have not or could not be undertaken. Follow these guidelines to help minimise the potential for disputes.

Recording Mail and Telephone Order Transactions

Records of each mail, telephone and Internet orders should provide:

- Cardholder's name (as it appears on the card)
- Cardholder's address (not a PO Box)
- Cardholder's signature (if mail order)
- Type of card (Mastercard and Visa)
- Card number (first four and last six digits only)
- Card valid from/to dates
- Authorised dollar amount(s) to be debited
- Period that standing authority (if any) is valid
- Contact telephone number
- Details of the goods or services required
- Transaction date
- Obtain authorisation for all orders
- Verify the delivery address and order details
- Check the delivery details to verify the name, address and telephone number
- Telephone the customer to confirm the order.

When the transaction has been processed and verified, promptly dispatch the goods.

6. Debit Card Transactions

The following procedures are vital in helping you identify and minimise fraudulent debit transactions via your merchant facility.

EFTPOS Debit Transactions are to be processed by swiping the presented card and having the customer enter their Personal Identification Number (PIN).

If you are unable to process a Debit Transaction due to a terminal communications or system failure, you must report the failure to ANZ Worldline Payment Solutions immediately and obtain authorisation to process the Debit Transaction manually.

Before manually processing any other Debit Transactions, you must swipe the Cardholder's card through the terminal to check if the failure has been rectified.

Manual Processing

This process is only to be used when the EFTPOS terminal communications or systems are unavailable or not working. Under no circumstances is a Debit Transaction to be processed as a manual transaction where the card's magnetic stripe is damaged or unable to be read by the Electronic Terminal.

Important:

Use the correct paper voucher system for the type of card being used and account being accessed. Please refer to the Manual Processing section located in your Merchant Operating Guide or contact ANZ Worldline Payment Solutions on 1800 039 025 for more information on manual processing.

Record your Authorised Floor Limits in the space provided at the front of your Merchant Operating Guide and obtain authorisation for all transactions over your Authorised Floor Limit. A manual Debit card voucher is NOT to be prepared when the terminal error message indicates:

- Declined Call Your Bank
- Tran Cancelled Card Error Refer
- Card Not Accepted
- Invalid Expiry Date

7. 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 employees account.

How to safeguard against this:

- Strictly control the access to your Merchant Card (where required to perform a refund) ensuring only authorised staff have access
- All refunds through your EFTPOS terminal should match with a corresponding sale on the same card
- Print and check your daily summary from the terminal to help identify large/unusual refunds you are not aware of
- Always balance EFTPOS settlement and refunds.

8. Third Party Transactions

A merchant should never process sales through their EFTPOS facility on behalf of another business or person. Not only is this a breach of your Merchant Services General Conditions, but it poses a significant risk to your business in the following ways:

Customers can dispute transactions and your business may be liable. A few reasons these sales could be disputed include:
- Fraudulent transactions
- They don't recognise your business name
- They didn't receive the goods/service from the business you processed the sales on behalf of

You may be in breach of Scheme (Visa & Mastercard) rules and be open to possible fines

You may be unwillingly processing, and becoming involved in, fraud

Your Merchant facility may be terminated.

9. Securing Your EFTPOS Terminal

Fraud and misuse of Credit or Debit Card information is a growing problem for many merchants globally. The loss of Customer Card data and subsequent misuse may undermine customer confidence and potentially reduce card usage at your business.

As part of ANZ Worldline Payment Solutions' ongoing commitment to providing the most up to date information on EFTPOS terminal and cardholder data security, we have outlined a list of Best Practices for protecting your terminals and your customer's information.

Your EFTPOS terminal is equipped with a number of in-built security features which are 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)
- Ensure that only authorised employees have access to your EFTPOS terminals and are fully trained on their use
- When closing your store or kiosk, 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 ANZ Worldline Payment Solutions. Be aware of unannounced terminal service visits
- Only allow authorised ANZ Worldline Payment Solutions 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, to ensure that the terminal casing is whole with external security stickers remaining unbroken and of a high print quality
- Ensure that there are no additional cables running from your EFTPOS terminal
- Remember to update your software to the latest version
- Make sure that any CCTV or other security cameras located near your EFTPOS terminal(s) cannot observe Cardholders entering details.

It is important to notify ANZ Worldline Payment Solutions (24 hours / 7 days a week) on 1800 039 025 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 ANZ Worldline Payment Solutions 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.

More information and training material on terminal and data security is available for you to download at anzworldline.com.au/merchant-security.

10. PCI DSS and Data Storage Requirements

What is the Payment Card Industry Data Security Standard (PCI DSS)?

PCI DSS is a set of standards implemented by the Card Schemes, Mastercard – Site Data Protection (SDP), and Visa – Account Information Security (AIS), to manage the risk to merchants of data breaches or hacker access. The standards apply to all merchants who store credit card data in any formation, have access to credit card details, or have systems which enable internet access to their company by the public.

Benefits to your business

- Ensuring the security of cardholder data can lessen the likelihood of a data breach resulting from your business
- Your business may experience improved patronage due to customers' confidence in the secure storage of vital information
- Helps to identify potential vulnerabilities in your business and may reduce the significant penalties and costs that result from a data breach.

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.

Remember - Don't store any cardholder data unless it is essential to your business

Key areas of focus

PCI DSS covers the following six key principles:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy.

What you need to do

Mastercard and Visa have created a set of tools and resources to assist you to implement the PCI DSS. Visa's program is called Account Information Security (AIS). Mastercard's program is called Site Data Protection (SDP).

For more information on working towards PCI DSS compliance, visit the PCI Security Standards Council website at pcisecuritystandards.org/index.shtml

Storage of prohibited cardholder data

As a merchant, it is vital to protect your customers as well as your business against misuse of credit & debit account information. It is essential that you do not store prohibited cardholder data such as magnetic stripe data (track data) and Customer Verification Value (CVV) after a transaction is completed.

Specific data such as a cardholder name, account number and the expiration date may be stored, but only if stored in accordance with the Payment Card Industry Data Security Standard (PCI DSS).

Prohibited cardholder data including magnetic stripe data (track data), and Customer Verification Value (CVV) must not be stored after a transaction is complete. For more information into storage of prohibited data and processing procedures, please visit visa-asia.com/secured.

11. Chargebacks and Retrievals

Chargebacks can have a financial impact on your business. It is important that you are fully aware of your obligations, the processes involved and possible outcomes. Please take the time to read through this carefully.

What is a Retrieval Request?

ANZ Worldline Payment Solutions will issue a Retrieval Request letter to you when a Cardholder or the Cardholder's issuing bank requires a copy of the receipt/voucher that has been processed.

What is a Chargeback?

A Chargeback is the term used for debiting a merchant's bank account with the amount of a transaction that had previously been credited. There are a number of reasons why a transaction may be charged back, but they mainly fall into two categories:

- Where the merchant has made an error at the point of sale;
- The cardholder or the card issuer is disputing the transaction. For example, the card or cardholder was not present at the point of sale,

or the cardholder does not recognise a transaction that has appeared on their statement. Under Condition 11 in the General Conditions of your Merchant Agreement, you may be charged back for the value of a transaction if that transaction is an "Invalid Transaction" as defined under the Agreement.

Chargebacks can occur for a number of reasons including a scenario where a Cardholder or their issuing bank justifiably disputes liability for the transaction for any reason or where the Merchant fails to comply with its obligations under the Merchant Agreement in connection with the transaction.

A Chargeback will also occur if a Retrieval Request is left unanswered or returned out of time by the merchant or if the supporting documentation supplied to the issuing bank is not acceptable.

In most cases, the value of the disputed transaction will be automatically debited from the merchant's account.

Common reasons for Chargebacks

- Processing errors
- Unauthorised use of a card
- No signature on the receipt
- Unauthorised transactions
- Invalid card account number
- Transaction exceeds floor limit
- Card details not imprinted on the sales voucher
- Incorrect transaction amount
- Expired card
- Transactions performed on a lost or stolen card
- Illegible details on the sales voucher
- Failing to respond to a retrieval request
- Merchandise not received by purchaser or wrong goods sent.

Note: This is not an exhaustive list of the circumstances in which a transaction may be charged back to you. You should refer to the General Conditions of your Merchant Agreement and to your Merchant Operating Guide for further details.

12. Transaction Evidence Request Letter

When a Cardholder disputes a transaction, the Cardholder's bank will send a **Transaction Evidence Request** or **Transaction Evidence for Chargeback** letter to the merchant requesting transaction evidence such as a signed transaction receipt.

The Merchant must provide information about a transaction which is requested by ANZ Worldline Payment Solutions within the timeframe specified by ANZ Worldline Payment Solutions in its request or, if no timeframe is specified, within ten (10) Business Days of the Merchant's receipt of the request.

Procedure:

Place all transaction evidence into the pre-paid envelope provided or fax to the number specified on the letter. Please note that all faxes must be clear and legible otherwise they may be rejected.

Should you experience difficulties locating the Transaction Voucher, please contact ANZ Worldline Payment Solutions on 1800 039 025 prior to the expiry period.

The following outcomes may follow from a Transaction Evidence request:

Outcome 1: If the Transaction Evidence Request letter and requested information is received by ANZ Worldline Payment Solutions within the date specified, it is forwarded to the Cardholder's bank to be reviewed. If the information is accepted by the Cardholder's bank without further issue, no further action is required.

Outcome 2: If the Transaction Evidence Request letter is received by ANZ Worldline Payment Solutions within the date specified, the information is forwarded to the Cardholder's bank and is reviewed against the Cardholder's dispute. If it is found that the merchant incorrectly processed the transaction (eg. no Cardholder's signature), the funds will be returned to the Cardholder from your merchant account.

Outcome 3: If the Transaction Evidence Request letter is not received by ANZ Worldline Payment Solutions within the date specified, ANZ Worldline Payment Solutions must advise the Cardholder's bank that no information was provided. The funds will be returned to the Cardholder from your merchant account.

Note: If a merchant responds late or fails to reply to a request for transaction evidence, it will result in a debit to the merchant account for the amount of the relevant "disputed" transaction that is not defended. It is imperative to respond to such requests in a timely manner to avoid this outcome.

Important:

If evidence is requested for a mail, telephone or Internet transaction, you must supply as many items of reference as you have relating to the transaction process, the customer and the product/service delivery.

13. Chargeback Adjustment Letter

The Cardholder's bank may request a Chargeback to the merchant. Once ANZ Worldline Payment Solutions has analysed the request and verified that all requirements for the requested Chargeback have been met, ANZ Worldline Payment Solutions will process the Chargeback to the merchant's account and the merchant will be sent a **Chargeback Adjustment** letter. That letter is sent to notify you that ANZ Worldline Payment Solutions has processed an adjustment to your account. The adjustment letter is generated and sent within one business day of the debit being processed.

14. Where to send Transaction Evidence

ANZ Worldline Payment Solutions
Merchant Chargebacks
Locked Bag 10
Collins Street West
Melbourne VIC 8007

Or

Fax **1800 156 113**

15. Frequently Asked Questions - Chargebacks and Disputes

How long should I keep my transaction vouchers?

You should retain copies of your transaction vouchers for at least 30 months. This is a requirement of the various card schemes including Mastercard and Visa.

What if the transaction was authorised?

Authorisation of a transaction does not amount to a representation or warranty that a transaction is genuine nor does it mean that the transaction will not be subjected to a Chargeback. Authorisation only verifies that the relevant card account is open and there are sufficient funds available in the account to meet the transaction amount. It does not guarantee that the person using the card is the authorised Cardholder.

Note: It is important to remember that all mail/telephone and other "card-not-present" transactions carry an inherent Chargeback risk. A chargeback can be defended in some instances.

If the dispute is raised in cases such as goods not received or credit not processed, then these can be defended.

If the transaction has been processed via Verified by Visa or Mastercard SecureCode, these cannot be raised as fraud by the Issuing bank and the issuing bank will be liable for these transactions if they have approved them.

If a cardholder raises a dispute for card not present fraud (e.g. hand-key transactions where the card is not physically presented), then it is almost impossible to defend.

Merchants should always respond to our requests for information as sometimes disputes are raised and it turns out to be another member of the family who has ordered online or via the phone and they will recognise it if information is provided.

If you are unable to satisfactorily substantiate the transaction, the liability for the transaction will lie with the merchant.

What should a merchant do when they receive a Retrieval Request?

Reply promptly within the timeframe specified on the request letter. Fax or send by post the requested documentation to ANZ Worldline Payment Solutions.

Note: Fax or send by post all relevant supporting documentation for that transaction including:

- Signed sales receipt
- Method of shipment
- Sales record, invoice or order form
- Signed delivery receipt and any other written confirmation of delivery
- Brief letter stating what occurred with the transaction.

What should a merchant do when they receive notification of a Chargeback?

Provide information about a transaction which is requested by ANZ Worldline Payment Solutions within the timeframe specified by ANZ Worldline Payment Solutions in its request or, if no timeframe is specified, within ten (10) business days of the Merchant's receipt of the request.

Note: Fax or send by post only the relevant documentation for that transaction including:

- Signed sales receipt
- Method of shipment
- Sales record, invoice or order form
- Signed delivery receipt
- Other applicable supporting documentation including a copy of the relevant guest register, folio or car rental agreement with a copy of the imprinted voucher signed by the Cardholder.

What Chargeback reasons am I protected against if I have implemented 3D Secure in my online payment facility?

Implementing 3D Secure in your online payment facility may help protect your business against the following Chargeback reasons:

- Reason Code 10.4 (fraud – card absent environment) - VISA
- Reason Code 37 (no cardholder authorisation) - Mastercard.

You are still expected to respond to all Chargeback retrieval request from ANZ Worldline Payment Solutions.

What should a merchant do when they have issued a credit refund to the Cardholder and still receive a Chargeback?

Fax a copy of the credit refund documentation that was previously processed to the Cardholder's account. Process credits each day and ensure that you always follow the instructions contained in the "Processing a Refund" section of your Terminal Guide when processing a refund.

What should a merchant do when a Cardholder states that the goods or services provided were defective and returns the goods to you?

Credit the Cardholder's credit card account or replace the goods.

Note: A Chargeback could be exercised after 30 days has elapsed.

What should a merchant do when a Cardholder who placed a mail telephone or Internet order states that they have not received the goods?

Obtain and retain proof of delivery to the Cardholder or to an authorised person accepting delivery on behalf of the Cardholder. Where relevant, ensure that you have the Cardholder's signature on a delivery receipt.

If you receive a Chargeback, forward this documentation when requested.

What should a merchant do when the terminal does not read a credit card?

Do not hand-key the Cardholder's credit card details.

Note: Only authorised mail, telephone and Internet merchants are able to hand-key details of a Cardholder's credit card.

- Prepare and complete a manual sales voucher with an imprint of the Cardholder's credit card. Ensure the transaction receipt includes a legible imprint of credit card number, name on the credit card and expiry date
- Telephone for authorisation and obtain an authorisation number
- Ensure the Cardholder signs the sales voucher.

What extra precautions can a merchant who accepts Mail, Telephone or Internet orders take to avoid Chargebacks?

- Always obtain authorisation for any transaction by contacting the appropriate provider and seeking an authorisation number
- Advertise under and process through the same business/trading name
- Have your business/trading name prominently displayed on the receipt
- Always include a receipt to the Cardholder
- Reply promptly to a retrieval request
- Obtain authorisations for transactions before shipping any goods (If the authorisation expires before shipping the goods, obtain a new authorisation and the Cardholder's signature)
- If the purchase involves recurring payments, make sure that the Cardholder is aware and obtain their signed consent to process Recurring Transactions

- If the payment is to be recurring over a period of time, ensure the card remains valid for the duration of that time period or contact the Cardholder for the revised expiry date should the card expire
- Make sure the transaction is processed between the valid dates on the card
- Obtain the billing and shipping address
- Obtain the Cardholder's telephone number and contact them when goods are to be shipped to reconfirm the transaction
- Do not deposit the funds from the sale until you forward the goods
- Mail an order confirmation notice prior to shipping
- Deposit sales vouchers within appropriate timeframes
- Ensure you are not getting multiple orders from the same card
- For Internet sales, ensure you are not obtaining multiple orders from the same email address
- When processing a refund, always follow the instructions contained in the "Processing a Refund" section of your Terminal Guide
- Encourage the use of security tools including Card Verification Codes, Mastercard SecureCode and Verified by Visa.

Remember:

It is your responsibility to inform staff of the above information. You are responsible for all transactions processed under your merchant facility so be sure to educate all staff members.

ANZ WORLDLINE
Payment Solutions

anzworldline.com.au

Item No. AW2004 09.2022 WZ123220 200.0112.02_AUS_EN/09.2022