

Manual Processing

Merchant Operating Guide



Contents

| 1. | Welcome | 4 |
|-----|--|----|
| 2. | Important Contact Details | 4 |
| 3. | Floor Limits and Authorisations | 5 |
| 4. | Fraud Minimisation | 6 |
| 5. | Security Tips for Mail, Telephone and Internet Order Merchants (for approved Merchants only) | 7 |
| 6. | Processing a Sale | 8 |
| 7. | Processing a Refund | 8 |
| 8. | Banking Vouchers | 10 |
| 9. | Errors and Disputes | 11 |
| 10. | Security of Information | 12 |
| 11. | Stationery | 13 |
| 12. | Change of Business Details | 13 |

1. Welcome

We are excited to welcome you as an ANZ Worldline Payment Solutions Merchant and look forward to a long association with you. This operating guide provides you with information about processing and banking credit card transactions manually, obtaining Authorisation and fraud prevention. Please take time to read this manual thoroughly and ensure that your staff read it too.

MERCHANT AGREEMENT

Your ANZ Worldline Payment Solutions Merchant Operating Guide contains valuable information and important requirements relating to the operating procedures for your Terminal. Instructions in this Guide form part of your ANZ Worldline Payment Solutions Merchant Operating Guide and may be changed or replaced by us in accordance with the terms of the merchant agreement.

ANZ Worldline Payment Solutions strongly recommends that you follow the security checks and procedures in this guide. These checks and procedures will assist you in identifying and minimising fraudulent, invalid or unacceptable

ANZ Worldling Dayment Solutions

transactions. Your Merchant Agreement sets out, in detail, the circumstances in which you will be liable for such transactions. You should read your Merchant Agreement carefully.

ANZ Worldline Payment Solutions may conduct an investigation if a Transaction is believed to be fraudulent. The operators of the applicable card schemes may also conduct their own investigations.

If it is found that you have processed invalid or unacceptable transactions you may also be liable for the value of those transactions. See your Merchant Agreement for more details.

2. Important Contact Details

1800 039 025 (24/7)

| 7.1.12 Tronamio i ajinoni oolationo | | | |
|--|--|--|--|
| E-mail | merchant@worldline.anz.com | | |
| Online Stationery Ordering | anzworldline.com.au or 1800 039 025 (OPT 1, 1) | | |
| Manual Authorisations | | | |
| Mastercard® and Visa | 1800 999 205 (Option 1) | | |
| Note: Calls to a 1800 number from a mobile phone will incur normal mobile phone charges. | | | |
| Merchant Details | | | |
| Merchant Number (please quote last 7 digits when calling) | | | |
| | | | |
| Floor Limits | | | |
| Mastercard \$ | | | |
| Visa \$ | | | |
| | | | |

3. Floor Limits and Authorisations

A Floor Limit is a dollar amount set for a particular type of card Transaction processed via your Merchant Facility. Your Letter of Offer outlines the Floor Limit specific to your business. When processing a Transaction manually which is over your Authorised Floor Limit, you must phone the Authorisation Centre to verify that the account has sufficient funds available to cover the Transaction. If you do not obtain approval for transactions above your Authorised Floor Limit, you risk the Transaction being dishonoured (charged back). Please remember that "Authorisation" does not amount to verification that the Transaction is genuine.

"Authorisation" of a Transaction by ANZ Worldline Payment Solutions does not mean authentication of the customer. Authorisation only confirms that the card number is a valid card number and that there are sufficient funds in the account. Authorisation does not prevent the Transaction being charged back if, for example, the credit card details were stolen and the true cardholder disputes the Transaction.

Despite a Transaction being "Authorised", the merchant bears the risk that the customer is not the true cardholder. Important points to remember are:

- Authorisation of the Transaction does not mean that the true cardholder has authorised the transaction;
- Authorisation does not protect the merchant from Chargeback; and
- the bank cannot guarantee the Transaction is being conducted by the true cardholder.

Please note that a Transaction may still be dishonoured (charged back) for other reasons even if approval has been given by the Authorisation Centre.

For example:

- when the card is not present and a Transaction is processed without the cardholder's permission or
- where you did not obtain an imprint of the card (manually or electronically) on the Transaction receipt.

When you contact the Authorisation Centre to authorise a Transaction, it will either be approved or declined. If the Transaction is declined, please advise the customer to contact the card Issuer (bank that issued the card) and seek an alternative method of payment.

AUTHORISATION DECLINED

If you are told not to accept a card, seek an alternative method of payment.

If the customer cannot pay by card or by an alternative means of payment, reclaim the goods where possible. If the goods cannot be reclaimed (eg. food items), take a description of the person or ask them to provide photographic identification such as a driver's licence. If unsuccessful in reclaiming the goods or securing an alternative method of payment from the customer, report the incident to the Police.

CANCELLING AN AUTHORISATION

An Authorisation reduces the available funds on a cardholder's card so you should cancel a Authorisation when your customer does not proceed with a sale. You can cancel a Credit card Authorisation by calling 1800 999 205 (option 3).

4. Fraud Minimisation

The following procedures are vital in helping you identify and minimise fraudulent credit card transactions processed through your Merchant Facility.

Before Commencing any Transaction:

- Confirm that you are authorised to accept that particular card
- Check to see if the card appears damaged or altered.

Card Front:

- Ensure that the name on the card is appropriate to the customer. Identity theft may have occurred if you are presented with a card containing the name of a cartoon character, a feminine name on a card presented by a male or other questionable scenarios
- The printing on the card should look professional
- The card must have 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)
- Cards should look 3-dimensional and contain familiar security features such as a hologram, signature panel and CVC (explanation to follow). It should not appear suspicious or be made of inferior material.

Note: A merchant is not permitted to process a manual Transaction on an unembossed credit card as they run the risk of the Transaction being dishonoured (charged back).

DURING THE TRANSACTION

Check the signature:

- · 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.

Be Alert for Customers Acting Suspiciously or Who:

- Appear nervous, overly talkative or in a hurry
- · Arrive at 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
- Make purchases without regard to size, quality or price of goods
- · Ask for transactions to be split
- Ask for the Transaction to manually entered
- Sign the voucher or Transaction voucher slowly or unnaturally.

Other Ways to Help Safeguard

- Do not let anyone service or remove your equipment without first providing adequate identification
- If you make an imprint of the card, make sure the black carbon sheets are destroyed
- Hold on to the card until you have completed the security checks and obtained authorisation for the transaction.

What To Do if You are Suspicious

 Ask for photographic identification (eg. a driver's licence or passport) and check that the details match the cardholder's name. Record the details on your copy of the Manual Transaction voucher or the printed Transaction voucher.

SPLIT TICKET TRANSACTIONS

The Transaction is invalid and may be charged back to the Merchant if, in ANZ Worldline Payment Solutions' reasonable opinion, the Transaction relates to one or more purchases made in the same Merchant establishment which have been split into two or more transactions in an attempt to avoid your Authorised Floor Limit.

DAMAGED CARDS

Damaged credit cards can be processed at your discretion, however, the risk of processing damaged cards remains with you as the Merchant.

When processing a sale with a damaged credit card, always seek Authorisation (even if the sale is under the Floor Limit).

ANZ Worldline Payment Solutions will not honour a Transaction when a damaged card is found to be invalid

When the sale is Authorised, record the Authorisation Number on the voucher, review information that proves the true identity of the customer and record the details on the sales voucher eg. driver's licence number.

Refer the customer to their card Issuer to arrange for a replacement card.

CARDS LEFT AT PREMISES

From time to time customers may accidentally leave their debit or credit cards behind at your premises. To ensure any potential fraud is minimised and to better align with broader industry practices, a change to existing handling process is required. Upon discovering a card left at your premises, you are to perform the following tasks:

- Retain the card in a safe place for a period of up to two business days;
- Hand the card to the customer claiming the card only after having established the claimant's identity by comparing signatures; and
- If the requisite two business days have passed, destroy the card.

Should the cardholder enquire about their missing card, instruct them to contact their issuing institution

5. Security Tips for Mail, Telephone and Internet Order Merchants (for approved Merchants only)

Note: Where an Authorisation is obtained for a Transaction, it does not guarantee that the Transaction is being made legitimately by the customer. An Authorisation on a Mail, Telephone (MOTO) or Internet Order Transaction may be Authorised on a card or card number which has been stolen or fraudulently used.

The following procedures are vital in helping you identify and minimise fraudulent credit card transactions.

- Obtain the credit card number, expiry date, customer's full name, address and contact telephone number
- · For telephone orders, record the name of the caller
- Do not accept an order or process a Transaction from anyone other than the cardholder
- Obtain Authorisation for all Transaction amounts over your Authorised Floor Limit
- Obtain an Authorisation if you have any doubts about a Transaction
- Check the telephone directory to verify the customer's name, address and telephone number
- For telephone orders, wait for a short period of time after the call is terminated, call the given contact telephone number and ask for the caller. Confirm the details of the order and record the date and time that you spoke with the person
- If a person who has ordered goods by telephone or over the Internet notifies you that they will be attending your premises to pick up the goods, advise them that they will be required to present their credit card to you at the time to confirm the details given by telephone or over the Internet. Take an imprint of the card and obtain a signature when it is presented
- Ensure deliveries are always made by your courier or a reputable courier engaged by you rather than your customer

- Ensure that the person making the delivery delivers the goods to a person inside the delivery premises or that the person collecting the goods comes from inside the premises. The person making the delivery should also obtain the signature and printed name of the person who accepts the delivery of the goods. Delivery couriers should be suspicious of people who approach them outside a delivery address eg. on a veranda when they arrive at the address or if they are met outside on the footpath
- Where delivering to company premises, ensure that the person accepting the delivery is an employee of the company. Request proof of identity and obtain a signature
- Deliveries should not be made to parks, carparks or public places
- Deliveries should not be left at unattended premises
- Deliveries should not be made to hotels, motels or Post Office boxes
- Provide your customer with a receipt number for the Transaction and maintain a record of that receipt number for at least 30 months
- Extra caution is necessary when dealing with orders from overseas
- For transactions you consider to be high value, it may be prudent to request the customer to fax the front and back of their credit card to you as well as suitable identification such as a driver's licence.

Adopting some or all of these suggestions does not guarantee that you will avoid credit card fraud. Your liability for credit card fraud is detailed in your Merchant Agreement.

If you are suspicious of any transactions, contact the Authorisation Centre shown in this guide prior to dispatching the goods.

6. Processing a Sale

- Perform security checks described in section 4
 Fraud Minimisation
- · Imprint the customer's card onto the sales voucher
- Remove the cover sheet as well as its attached carbon and destroy
- Check that the imprinted details are clear
- · Complete the voucher entering the final amount
- Have your customer sign the youcher
- Compare the signature on the voucher with that on the card.

If they do not match, do not complete the Transaction and seek an alternative form of payment. Contact the Authorisation Centre on 1800 999 205.

Remember to seek Authorisation for all purchases over your Floor Limit.

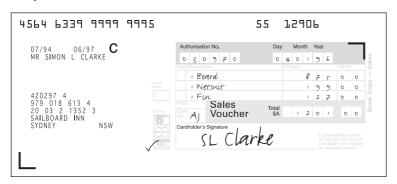
Reminder: A merchant is not permitted to process a manual Transaction on an unembossed credit card as they run the risk of the Transaction being dishonoured (charged back).

To Obtain Authorisation, Contact the Authorisation Centre

If the Transaction is approved, record the Authorisation Number on the voucher.

If the Transaction is declined, seek an alternative method of payment and advise the customer to contact their card Issuer.

When the Transaction is in order, hand the customer the yellow (Customer) copy of the voucher and their card. Retain the Merchant copy for your records and the Bank copy for banking.



7. Processing a Refund

If a refund is required on a Transaction which has not been processed, you must cancel the Authorisation if already obtained. Refer to section 3 Floor Limits and Authorisations for details on how to cancel an Authorisation.

Refunds are easy to process if a customer returns goods purchased from you or for services terminated or cancelled.

VISA AND MASTERCARD

For any goods purchased with a Visa or Mastercard scheme card that is accepted for return, or for any services that are terminated or cancelled, or where any price adjustment is made, you must first attempt to process the refund (credit transaction) to the same card that was

used for the original purchase transaction.

If the card that was used for the original purchase transaction is not available (e.g. it is expired) and therefore a refund is required to be processed by other means, please ensure you keep all supporting documentation to show:

- · the method used to refund;
- · the cardholder contact details: and
- · details of the original purchase.

This is in order to provide evidence if a chargeback claim is submitted. However, this does not guarantee you will not be liable in the event of a chargeback claim.

Provided that you have adequate supporting documentation proving that the original purchase

transaction took place on the original card, you may process the refund onto an alternate card, which belongs to the same cardholder as the card used for the original purchase transaction, under any of the following types of circumstances:

- The original account is no longer available or valid (for example, the original card has been replaced due to expiration or being reported lost or stolen)
- The authorisation request for the refund transaction was declined by the issuer.

When a refund cannot be processed to the original card or to an alternate card, and provided that you have adequate supporting documentation proving that the original purchase transaction took place on the original card you may offer an alternate form of refund (for example, cash, cheque, in-store credit, prepaid card, etc.), under any of the following types of circumstances:

- The refund is made to a recipient of a gift (instead of to the cardholder who made the original purchase)
- The original sale took place on a Visa or Mastercard prepaid card, which has since been discarded
- The authorisation request for the credit transaction was declined
- In order to comply with any applicable Laws, including but not limited to the "Australian Consumer Law", as set out in Schedule 2 of the Competition and Consumer Act 2010 (Cth) (Australian Consumer Law).

OTHER CARD SCHEMES

For any goods purchased with a card belonging to schemes other than the Visa or Mastercard schemes, that is accepted for return, or for any services that are terminated or cancelled, or where any price adjustment is made, you must not make either any cash-based refund to the cardholder or a refund to another card number unless you are required to do so in order to comply with any applicable Laws, including but not limited to the Australian Consumer Law. If you do so, you may be liable for a chargeback should a cardholder dispute the original sales transaction, which may result in a debit to your Merchant Account for the relevant "disputed" transaction.

If a refund transaction is performed on an international card, please advise the cardholder that the refund amount displayed on their statement may vary from the purchase amount due to the changes in currency exchange rates.

To process a refund using a Transaction Voucher (credit voucher), you should:

- · perform security checks
- imprint the customer's card onto the credit voucher
- remove the cover sheet and its attached carbon and destroy
- check that the imprinted details are clear
- · complete the voucher
- · sign the voucher to Authorise the refund
- hand the customer the yellow (Customer) copy of the youcher and their card
- retain the Merchant copy for your records and the Bank copy for banking.



8. Banking Vouchers

To receive value for your credit card transactions, you must deposit the Bank (white) copies of vouchers with a completed credit card Merchant Summary voucher or MOTO Transaction record within three business days of the date of the transactions.

Preparing Your Deposit

 If possible, produce an adding machine tape showing the value of each Sales and Credit voucher and the total value of the vouchers (or write up to 8 voucher values directly onto Merchant Summary)

No more than 50 vouchers can be banked with any one Merchant Summary voucher

- Imprint your ANZ Worldline Payment Solutions Merchant Summary card on a Merchant Summary voucher
- · Complete the voucher.

Place into your Merchant Summary envelope:

- · Bank copies of all Sales and Credit vouchers
- Bank copy of Merchant Summary voucher
- · Adding machine tape (if any).

Do not pin, staple, clip or fold the envelope contents.

Do not include cheques, cash or other card scheme vouchers eg. American Express, Diners Club or JCB as ANZ Worldline Payment Solutions cannot process these card types.

 Complete your normal bank deposit slip. Record the net amount of your credit card Merchant Summary on the last line of the cheque listing and add it to the total of cheques.

Merchants with an ANZ bank account:

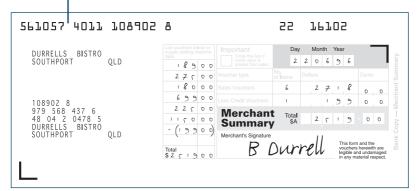
Please deposit the completed Merchant Summary Envelope at any ANZ branch.

Merchants with a non ANZ bank account:

Please send the completed Merchant Summary Envelope with your completed non ANZ bank deposit slip to:

Not for Value Merchant Envelopes Settlement and Control Team Tower 4, Level 15, Collins Square, 737 Collins Street. Melbourne VIC 3000

Full merchant number is to be imprinted on Merchant Summary



IMPORTANT: Make sure that the envelope contains only credit card vouchers.

ENVELOPES WHICH HAVE A CREDIT VALUE

When the value of credits is greater than sales, enter an 'x' in the box on front of Merchant Summary envelope. When you bank the vouchers, hand the teller cash or cheque(s) to the value of the net credit amount.



9. Errors and Disputes

Vouchers from credit card transactions which cannot be processed are debited from your bank account and returned for correction. This is known as a Return and Correction (R&C) but may also appear on your Merchant Statement as MTL (Monetary Transmission Log).

Typical Causes of R&Cs are...

- Incorrectly completed vouchers (e.g. incorrect additions on Merchant Summary vouchers)
- Incomplete information (e.g. unreadable card imprint on voucher)
- Banking of vouchers from other schemes (e.g. American Express).

When you receive an R&C, there will be an explanation of why it cannot be processed. Make sure you rectify the problem before re-submitting the voucher for processing.

CHARGEBACKS

Please refer to the General Conditions of your ANZ Worldline Payment Solutions Merchant Agreement. You may be charged back for the value of a Transaction where you have failed to comply with your obligations as stated in this Merchant Operating Guide or otherwise included in the

General Conditions of your ANZ Worldline Payment Solutions Merchant Agreement.

Chargebacks can occur for a number of reasons such as:

- A Transaction has been processed using an invalid card (i.e. the card has expired or is not yet valid)
- A sale over your Floor Limit is processed without Authorisation
- A split sale is processed using two or more vouchers to avoid obtaining Authorisation
- A manual Transaction has been processed on an unembossed credit card
- A credit voucher was not processed for returned goods
- A sale is processed without the customer's signed authority.

A Transaction will also be charged back to you if a cardholder disputes a Transaction and you are unable to produce evidence to defend that dispute (for example, copies of the relevant Transaction Vouchers). If you need assistance understanding a particular Return and Correction or Chargeback, please contact ANZ Worldline Payment Solutions during business hours.

10. Security of Information

PCI DSS AND DATA STORAGE

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 being traced back to your business
- Your business will experience continued 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.

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 account information. It is essential that you do not store prohibited cardholder data 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 www.visa.com.au/support/small-business/security-compliance.html.

Do not divulge cardholder information (eg. card numbers) or allow equipment to be used by unauthorised persons.

FILING VOUCHERS

Make sure you keep your copies of all credit card Transaction vouchers or MOTO Transaction records and associated order details in a secure place for at least thirty months in case a Transaction is disputed.

For easy retrieval of vouchers, file them in Merchant Summary date order.

Check your Merchant Summary or MOTO total against your monthly ANZ Worldline Payment Solutions Record of Merchant transactions.

At the end of the 30-month period, you must destroy any cardholder data relating to the Transaction. You must ensure that any document containing any cardholder account number is securely destroyed in a manner which makes that information unreadable.

11. Stationery

ANZ Worldline Payment Solutions supplies you with:

- Imprinter
- · Sales and Credit Vouchers
- Merchant Summary Vouchers
- · MOTO pad (if authorised)
- Merchant Summary Envelopes
- Telephone stickers, window decals and other point of sale material
- · This Merchant Operating Guide.

To re-order ANZ Worldline Payment Solutions stationery, please order online at anzworldline.com.au or contact ANZ Worldline Payment Solutions on 1800 039 025 (Option 1). Allow up to 10 business days for delivery and remember to check your stationery levels regularly.

12. Change of Business Details

Your Merchant Agreement describes various situations in which you must notify us of a change to your circumstances. Please contact ANZ Worldline Payment Solutions on 1800 039 025 if there are any changes to your:

- · Business name and/or address
- Business type or activities including changes in the nature or mode of operation of your business
- Mailing address
- Bank/branch banking details
- · Telephone or fax numbers
- · Business ownership.

Should your business be sold, cease to trade or no longer require an ANZ Worldline Payment Solutions Merchant Facility, please contact ANZ Worldline Payment Solutions on 1800 039 025.

The ANZ Worldline Payment Solutions General Conditions sets out your obligations when your business is sold, ceases to trade or no longer requires an ANZ Worldline Payment Solutions Merchant Facility.

You must ensure that all stationery, promotional material, Transaction Vouchers, card Imprinters and equipment (including Electronic Terminals) is returned to ANZ Worldline Payment Solutions, based on the closure instructions provided by ANZ Worldline Payment Solutions.

Please Note: It is the authorised merchant's responsibility to ensure that the Merchant Facility is returned. Failure to do so, may result in the continual charge of Equipment Fees until all equipment is returned in accordance with condition 16(iv) of the ANZ Worldline Payment Solutions General Conditions.



About ANZ Worldline Payment Solutions

On 15 December 2020 Australia and New Zealand Banking Group Limited announced that it was setting up a partnership with Worldline SA to provide leading payments technology and merchant services in Australia

The joint venture formed by ANZ and Worldline SA is known as ANZ Worldline Payment Solutions and aims to give merchant customers in Australia access to Worldline SA's market-leading payments technology and future innovations. ANZ Worldline Payment Solutions commenced operations on the 1st April, 2022.

Pairing Worldline SA's global leadership with ANZ's local expertise and existing relationships, ANZ Worldline Payment Solutions aims to offer fast, reliable and secure point-of-sale and online payment acceptance for merchants and their customers in Australia, and strives to deliver a suite of competitive products and an innovative roadmap to help your business grow.

ANZ Worldline Payment Solutions means Worldline Australia Pty Ltd ACN 645 073 034 ("Worldline"), the provider of merchant solutions under the Merchant Agreement. Worldline is not an authorised deposit taking institution (ADI) and entry into the Agreement is neither a deposit nor liability of ANZ or any of its related bodies corporate (together "ANZ Group"). Neither ANZ nor any other member of the ANZ Group stands behind or guarantees Worldline.

Instructions appearing in this Merchant Operating Guide form part of your Merchant Agreement and may be varied or replaced by ANZ Worldline Payment Solutions at any time.

ANZ WORLDLINE W//. Payment Solutions