ANZ WORLDLINE
Payment Solutions

Merchant Operating Guide

Merchant Operating Guide

1. Welcome 2
1.1 Agreement 2
1.2 Important Contact Details 2
1.3 Authorisation 2
1.4 Floor Limits & Debit Cards Pin Limits 2
1.5 Change Of Business Details 3
2. Cards and Alternative Payment methods you can accept 3
2.1 Credit Cards 3
2.2 Debit Cards 3
2.3 Charge Cards 3
2.4 Alternative Payment Methods 3
3. Passwords 4
3.1 Forgotten Password 4
4. Equipment maintenance 4
5. Stationery 4
6. Fraud Minimisation 5
6.1 Card Present Card Checklist 5
6.2 Fraud Minimisation For Credit Cards 6
6.3 Fraud Minimisation For Debit Cards 7
6.4 Cards Left At Premises 7
7. Handling cardholder information securely and PCI DSS 7
7.1 Pci Dss – Payment Card Industry Data Security Standard 7
7.2 Securing Transaction Records 8
7.3 Chargebacks 8
8. Surcharge 9
9. Tipping 11
10. Cash Out and Purchase with Cash Out 11
11. Refunds 11
12. Referenced Refunds 12
13. DCC – Dynamic Currency Conversion 14
13.1 DCC Rebates 15
14. Mail Order Telephone Order (MOTO) 15
15. Pre-Authorisations 16

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 Merchant Operating Guide provides you with information on payment cards and mobile application payments you can accept, ways to reduce fraud and what to do if errors or disputes occur. Easy-to-follow instructions on how to process transactions via your ANZ Worldline Payment Solutions ElectonicTerminal are provided. Please take time to read this guide thoroughly and ensure your staff read it too.

1.1 Agreement

Your ANZ Worldline Payment Solutions Agreement contains valuable information and important requirements relating to operating procedures. Unless otherwise defined, Capitalised terms used in this Merchant Operating Guide have the same meaning given to them as in the ANZ Worldline Payment Solutions General Conditions (General Conditions). ANZ Worldline Payment Solutions strongly recommends that you follow the security checks and procedures in this guide to assist in identifying and minimising fraudulent, invalid or unacceptable transactions. ANZ Worldline Payment Solutions may conduct an investigation if a transaction is believed to be fraudulent. The operators of the applicable Nominated Card Schemes or Alternative Payment providers may also conduct their own investigations. Your Agreement outlines the circumstances in which you will be liable for such transactions. If it is found that you have processed invalid or unacceptable transactions, you may be liable for the value of those transactions. Please refer to the General Conditions for more details.

1.2 Important Contact Details

ANZ Worldline Payment Solutions (24 hours a day/7 days a week): 1800 039 025

Online Stationery Ordering: anzworldline.com.au/merchant-support

1.3 Authorisation

Your Electronic Terminal is designed to automatically seek authorisation from the cardholder's card/payment issuer while processing an electronic transaction.

Authorisation confirms that the card number is a valid card number and that there are sufficient funds in the account. Despite a transaction being 'authorised', the merchant bears the risk that the customer is not the true cardholder.

Authorisation does not amount to verification that the transaction is genuine nor does it authenticate the customer.

- Authorisation of the transaction does not mean that the true cardholder has authorised the transaction
- Authorisation does not protect the merchant from chargebacks
- ANZ Worldline Payment Solutions cannot guarantee that a transaction has been conducted by the true cardholder.

Authorisation Declined

Where an authorisation is declined, please seek an alternative method of payment

1.4 Floor Limits & Debit Cards Pin Limits

A Floor Limit is a dollar amount set for a particular type of card transaction processed via your Merchant Facility. Please note, an Authorised Floor Limit of $0 applies to manual, electronic and online payments for Visa and Mastercard cards.

Any transaction amount above the limits in the following table (not including Visa® and Mastercard® transactions) will require the cardholder to enter a Personal Identification Number (PIN) to verify the transaction:

MCC	Transaction type	Pin limit
a) All	Cash Out or Purchase with Cashout	$0
b) Service stations, taxis/limousines, liquor and convenience stores	Purchase	$60
c) Supermarkets	Purchase	$200
d) Other (excluding (b) and (c) above	Purchase	$100

A single transaction limit of $5000 USD per Transaction may apply to Unionpay International transactions on restricted merchant categories

1.5 Change Of Business Details

The General Conditions describe various situations in which you must notify us of a change to your circumstances.

Please visit https://anzworldline.com.au/en/ home/merchant-support.html to complete and submit the respective form or contact ANZ

Worldline Payment Solutions on 1800 039 025 if there are any changes to your:

- Legal entity name
- Business name
- Address(es) where you carry on business
- Business type or activities including changes in the nature, scope, type or mode of operation of your business
- Mailing address
- Ownership
- Bank/branch banking details
- Telephone number(s)
- Industry
- Email address.

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 General Conditions set 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 Electronic Terminals) are returned to ANZ Worldline Payment Solutions, based on the closure instructions provided by ANZ Worldline Payment Solutions.

Please note that it is the authorised merchant's responsibility to ensure that the any Electronic Terminals and other associated equipment are returned. Failure to do so, may result in the continual charge of Terminal Rental Fees until all equipment is returned in accordance with condition 19(iv) of the General Conditions.

2. Cards and Alternative Payment methods you can accept

2.1 Credit Cards

Cardholders can use credit cards (Visa, Mastercard and, subject to eligibility and relevant limits, UnionPay International) to

perform transactions through the ANZ Worldline Payment Solutions Electronic Terminal on their credit card accounts. Cardholders can also access cheque and savings accounts where those accounts are linked to the credit card. Cardholders can access these accounts through the ANZ Worldline Payment Solutions Electronic Terminal using their PIN and in certain

circumstances, their signature. Cardholders can also use their contactless card, smartphone or wearables to make the purchase by tapping the Electronic Terminal's contactless reader. For contactless transactions under a certain purchase value, PIN or signature may not be required to verify a transaction.

2.2 Debit Cards

Cardholders possessing a debit card will need to use a PIN for verification in most circumstances. A signature may also be requested. Cardholders can also use their contactless card, smartphone or wearables to make the purchase by tapping the Electronic Terminal's contactless reader. For contactless transactions under or equal to a certain purchase value, PIN or signature may not be required to verify a transaction. Please refer to section 1.4 for Debit Card PIN limits.

2.3 Charge Cards

To accept charge cards, you must have an agreement with the charge card issuer (e.g. Diners Club, American Express and JCB).

2.4 Alternative Payment Methods

If enabled, your customer can also pay using Alternative Payment Methods such as WeChat Pay, Alipay+, and the other digital wallets enabled in Australia through Alipay+. These payments are done by scanning the QR code that is displayed on your Electronic Terminal's screen.

3. Passwords

To restrict access to certain PINpad functions and processing of transactions, a default merchant password has been set on the Electronic Terminal. Access to the below functions cannot proceed until a valid password is entered when prompted by the Electronic Terminal. Please note passwords do not apply to integrated Electronic Terminals.

- Reversal
- Refund

Each Electronic Terminal you have will have a password and it is your responsibility to keep your password secure and only share it with authorised staff.

Unauthorised access to this password can result in unauthorised reversal or refund transactions via your Merchant Facility resulting in financial loss to your business.

To protect against fraud and prevent any unauthorised use:

- For each Electronic terminal, change your merchant password periodically, ideally at least every six months and/or after an authorised staff member has left your business
- Ensure only you and your authorised employees have access to your Electronic Terminals and passwords
- When processing transactions that require passwords, ensure there are no customers observing while you are entering your password
- Protect all passwords against unauthorised use
- Never save your password in an easily accessible location.

ANZ Worldline Payment Solutions will use your contact details for all the ongoing password related communications. To ensure you receive all the necessary communications, it is your responsibility to contact ANZ Worldline Payment Solutions to keep these details up to date for each of your sites.

3.1 Forgotten Password

If you have forgotten your Password, please contact ANZ Worldline Payment Solutions on 1800 039 025 any time, 7 days a week, to request a password reset.

Note: ANZ Worldline Payment Solutions will validate the caller by performing certain checks as advised as part of your onboarding. Should you require a staff member to request a password reset on your behalf, please ensure they have been provided with the relevant information

4. Equipment maintenance

It is your responsibility to provide a clean operating environment for your Electronic Terminal. Liquids and dust may damage the Electronic Terminal components and can prevent it from operating.

To prevent a fire, power units and cords should be inspected regularly. If any damage to the power units and cords are found on your

Electronic Terminal, please contact ANZ Worldline Payment Solutions on 1800 039 025 for assistance. It is important to clean your Electronic Terminal regularly to maintain its operating efficiency as you may be charged if it is damaged. The Electronic Terminal and screen may be wiped clean using a damp cloth. Do not use abrasive materials. Use a soft brush to keep the keypad dust-free.

- Please do not tamper with or remove the Electronic Terminal housing
- Do not place stickers on the Electronic Terminals
- Do not disconnect your Electronic Terminal's power supply or communication line unless

  instructed to do so by ANZ Worldline Payment Solutions.

5. Stationery

You have been supplied with an initial stock of stationery including:

- 8 x Paper rolls (for Electronic Terminals only)
- 1 x Door sticker (cards accepted)
- Terminal Quick Reference Guide (QRG)
- A fridge magnet with a links to our EFTPOS terminal support page, where you can access information / support for your Electronic Terminal on items such as:

- Fraud Minimisation, Data Security and Chargeback Guide
- General Conditions
- Alipay+ and WeChat Pay Information Guide
- Merchant Operating Guide (MOG)

To re-order stationery, please visit

anzworldline.com.au or contact ANZ Worldline Payment Solutions on 1800 039 025. Please only use the stationery approved by ANZ Worldline Payment Solutions.

6. Fraud Minimisation

Before commencing any transactions, please take time to read through the Fraud Minimisation,

Data Security and Chargeback Guide at anzworldline.com.au/merchant-support/200011202-ma-fraud-chargeback-guide-aus-en.pdf for further detailed fraud information to assist you in protecting your business.

6.1 Card Present Card Checklist

How to Safeguard Against Fraud:

- Do not let anyone service or remove your terminal without viewing proper identification
- Do not allow equipment to be used by unauthorised persons
- Keep Merchant Cards secure from unauthorised use
- Do not divulge cardholder information (e.g. card names or numbers)
- Retain the card until you have completed the security checks and obtained Authorisation for the transaction
- Do not locate your Electronic Terminal under a security camera or any other CCTV device.

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 distract you
- 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 to split transactions into smaller amounts
- Ask for transactions to be manually entered
- Sign the voucher or transaction voucher slowly or unnaturally.

If you are suspicious of a transaction, it is recommended you:

- Ask for photographic identification (e.g. driver's licence or passport) and ensure the details match the cardholder's name.

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 purchases)
- Please report all fraudulent activities to the police immediately.

Split Ticket Transactions

A transaction may be deemed invalid and charged back to you if, in ANZ Worldline Payment Solutions' reasonable opinion, it relates to one or more purchases made in the same merchant establishment which have been split into two or more transactions.

Chip Card Processing

Chip cards are embedded with a security microchip that provides further protection to assist in decreasing the risk of fraudulent transactions and chargeback disputes. As with any other transaction, a degree of caution must also be exhibited when processing chip card transactions.

For Card Present Transactions, look at the card and if there is a chip, always:

- insert the card into the chip reader at the first instance and follow the prompts; or
- in the case of a contactless transaction enable a contactless card to be read by your Electronic Terminal, otherwise swipe or insert it following any prompts including those indicating the need for a PIN and/or a signature.

If:

- The Electronic Terminal displays "Insert Chip" when the card is swiped through the Electronic Terminal and the card in question does not have a chip on it, do not proceed with the transaction
- The Electronic Terminal displays "Insert Chip" and the chip, when inserted, cannot be read by the Electronic Terminal, do not proceed with the transaction.

6.2 Fraud Minimisation For Credit Cards

The following checks are vital in helping you identify and minimise fraudulent credit card transactions via your ANZ Worldline Payment Solutions Merchant Facility.

Before commencing any transaction:

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

Check on the front of the card that:

- 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 Card Validation Codes such as; CVC, CVC2, CVV2 or CID which are the 3 or 4 digit number on the nominated card . It should not appear suspicious or be made of inferior material.

Note: Some UnionPay cards may be issued with zeros or no expiry date. These cards may still be valid.

Embossed cards

The cardholder name and number is raised and not flattened, unless it is a genuine un-embossed card. The embossing should be clear and even.

Unembossed cards

- A cardholder name may or may not be included
- Can only be used for electronic transactions
- The cardholder name and number are printed rather than raised.

Check the signature during the transaction:

- A signature should appear within the signature panel on the card
- The signature or signature panel should not appear to have been altered
- The customer's signature on the transaction voucher matches the signature on the card if a PIN is not used.

Card Validation Code (CVV2)

The card validation security feature is activated in all Worldline DX 8000 terminals when processing mail order and telephone order transactions.

Turn the cardholder's credit card over and locate the last three digits of the number printed on the signature panel. If the transaction is initiated via mail, telephone or internet, instruct the cardholder to locate and quote the three digits on the signature panel.

Note: American Express cards have a four-digit code located on the front of the card. Diners Club cards have a three-digit code on the reverse of the signature panel.

When the transaction has been processed, check:

- The card number details against those printed on the transaction record

- The trading name and address details are correct
- Ensure that 'Approved' or an approval number/code is printed on the transaction record.

6.3 Fraud Minimisation For Debit Cards

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

Debit transactions are to be processed by swiping or inserting the presented card and having the customer enter their PIN or, in certain circumstances, their signature.

6.4 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 viewing valid identification
- 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.

7. Handling cardholder information securely and PCI DSS

You are responsible for the security of all cardholder and transaction information you receive, process or store.

Businesses store credit card details for various purposes. While sometimes this is necessary to support legitimate business practices, storage of card data can lead to theft of customer information and significant impact to your business. ANZ Worldline Payment Solutions recommend card data is never stored on your systems.

7.1 Pci Dss – Payment Card Industry Data Security Standard

The PCI DSS is a global security standard developed by Visa®, Mastercard®, AMEX and other card schemes to ensure consistent security standards for all organisations that store, process or transmit cardholder information. Visa® and Mastercard® require all ANZ Worldline Payment Solutions merchants to be compliant with PCI DSS.

PCI DSS covers the following 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 are the benefits of PCI DSS compliance?

PCI DSS compliance may assist your business in protecting payment card data and minimising risk of theft of cardholder information or compromise of your business systems.

Maintaining a PCI DSS compliance program could help your business identify potential vulnerabilities and may reduce the financial penalties and remediation costs from a data breach.

Validating PCI DSS compliance

To validate compliance with PCI DSS, your business must complete the following validation tasks:

1) Annual PCI DSS assessment

The self-assessment questionnaire (SAQ) is a free assessment tool used to assess compliance with the PCI DSS standards. There are many different SAQs, covering a variety of payment processing environments, available to download from the PCI SSC website at:

https://www.pcisecuritystandards.org/document_library/

Compliance assessments may also be performed by completing an onsite audit with an independent PCI-approved Qualified Security Assessor (QSA). PCI maintains a list of PCI- approved QSAs at:

https://listings.pcisecuritystandards.org/ assessors_and_solutions/qualified_security_assessors

2) Quarterly network vulnerability scans

If your business accepts payments via the internet or has any electronic storage of cardholder or transaction information, then quarterly network vulnerability scanning is required to ensure compliance with PCI DSS.

An external vulnerability scan enables your business to assess your level of security from potential external threats.

PCI-approved scanning tools are used to generate traffic that tests your network equipment, hosts, and applications for known vulnerabilities. The scan is intended to identify vulnerabilities so they can be corrected.

ANZ Worldline Payment Solutions provides a complimentary PCI DSS Compliance Program to our merchants, including PCI-approved network vulnerability scanning – please email pci-compliance-ms-au@worldline.com to request access to our PCI DSS program.

7.2 Securing Transaction Records

In general, no cardholder data should be stored unless it is strictly for use within the business and absolutely necessary.

However, if you have authority from ANZ Worldline Payment Solutions to process MOTO or eCommerce transactions you may be required to store cardholder data and transaction records. Please ensure all paper and electronic records containing cardholder data are secured (e.g. locked filing cabinet), these may include: MOTO order forms, or pre-authorisation transactions.

Where storage of cardholder data is required, you must ensure both the type of cardholder data retained, and the method used to store it is compliant with PCI DSS and ANZ Worldline Payment Solutions requirements.

Here are a few simple guidelines:

- Never email credit card numbers or request your customers provide their credit card number by email
- Ensure you process eCommerce transactions with security codes (for e.g., CVV2/ CVC2), but do not store these codes after they have been authorised
- Keep cardholder data storage to a minimum, only what is necessary for business or legal needs
- Once a transaction is processed, obscure all digits except the first six and last four digits of the credit card number (e.g. 1234 56XX

  XXXX 7890) on all paper and electronic records
- Store cardholder data in a secure environment with strict controls and restricted access
- Use strong passwords which are changed at least every 90 days for all administrator roles and users with access your customer's card details
- Avoid storing cardholder data on PC's, laptops or mobile phones
- Do not store your customer's card details online or unencrypted on your computer
- Securely dispose of cardholder data as soon as its use has expired. PCI DSS recommends shredding, pulping, incinerating or other methods which make it impossible to reconstruct the cardholder data. ANZ Worldline Payment Solutions requires you keep transaction records for 30 months minimum
- Under no circumstances should sensitive information be stored; this information includes security codes (for e.g. CVV2, CVC2), PIN or magnetic stripe data.

The following sources provide guidance on card data storage:

- Refer to the General Conditions condition 38 for 'Information collection, storage and disclosure'
- For more information, visit the PCI Security Standards Council website at https://www.pcisecuritystandards.org/.

7.3 Chargebacks

A chargeback is the term used for debiting a merchant for the amount of a transaction that had previously been credited, in the circumstances outlined below. 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 time to carefully read through the Fraud Minimisation, Data Security and Chargeback guide at anzworldline.com.au.

You may be charged back for the value of a credit or debit card sale where you have failed to follow the procedures as stated in the General Conditions.

Note: You must retain information about a transaction for a period of 30 months from the date of the transaction or such other period required by card schemes, Law or notified by ANZ Worldline Payment Solutions. For an Alternative Payment Method, you must retain information about a transaction for a period of five years from the date of the transaction or such other period required by the Alternative Payment Method schemes, Law or notified by ANZ Worldline Payment Solutions.

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 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 as set out in the General Conditions.

Chargebacks can occur for a number of reasons, including:

- Processing errors
- Unauthorised use of a card
- 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: The examples given above are not an exhaustive list of the circumstances in which a transaction may be charged back to you. Please refer to the General Conditions or your Agreement for further information on chargebacks.

If you need assistance understanding a particular Return and Correction or chargeback, please contact ANZ Worldline Payment Solutions on 1800 039 025 (24 hours a day, 7 days a week).

8. Surcharge

The Reserve Bank of Australia (RBA) introduced Standard No 3 of 2016 (the "RBA Standard") on 1 September 2016 for Large Merchants (as defined in the RBA Standard) and on 1 September 2017 (for other relevant merchants). The objective of the RBA Standard is to promote efficiency and competition in the Australian payments system. It includes surcharging regulations for merchants who accept certain card scheme payments and choose to surcharge their customers for the cost of doing so.

Permitted surcharge costs are listed in the RBA Standard and include fees paid to the merchant's acquirer such as merchant service fees, card transaction processing fees and certain other observable costs paid to third parties for services directly related to accepting particular types of cards.

If you plan to surcharge, you should ensure that you and your staff are fully aware and informed of the detailed provisions of the RBA Standard. Compliance with the RBA Standard is your responsibility as a merchant.

A full copy of the RBA Standard (Standard No 3 of 2016) is available on the RBA website.

How much to surcharge?

Calculating the amount to surcharge is the responsibility of the merchant. Under the surcharging regulations, the amount you can surcharge customers (e.g. at the time of payment), must be limited to the reasonable cost to accept that card type transactions during a 12 month period which ended not more than 13 months ago. You will be able to use the information on your the Cost of Acceptance Report, that you will receive each month, to assist you.

In addition to acquirer fees, the surcharging regulations allow specific other costs to be recovered from a payment surcharge if they directly relate to the card type being surcharged. These costs may include:

- fraud prevention services
- direct gateway costs
- any Electronic Terminal costs paid to a provider other than the merchant's acquirer or payments facilitator
- switching fees, or
- insurance premiums for the provision of goods/services not being provided due to payments effected by card transactions.

These costs must be verifiable via contracts, statements or invoices. Costs internal to your business cannot be included in a surcharge.

How often do merchants have to review their surcharge amount?

Merchants in Australia are required to regularly review their surcharge amounts (a least once a year) to ensure that they are in compliance with RBA regulations and are not over-recovering their costs.

Additionally, if the RBA changes its regulations regarding the reasonable cost of acceptance, merchants should review their surcharge amounts to ensure they remain compliant.

Which cards do the RBA standards apply to? The standards currently apply to the following:

- Eftpos/Eftpos Prepaid,
- Mastercard Debit/Prepaid,
- Mastercard Credit,
- Visa Debit/Prepaid, and
- Visa Credit
- Other card systems may include conditions in their merchant agreements that are similar to the limits on surcharges under the RBA's standard, in which case merchants may be contractually bound to similar caps on what they can surcharge on cards from other systems. Over time other payment types could be added via regulation.

Is surcharging compulsory?

A merchant can choose to apply surcharge or not.

However, once a merchant decides to apply surcharging on their Electronic Terminal, they need to follow RBA and ACCC rules of not charging beyond the cost of acceptance.

Where to get further information on surcharging?

Merchants are advised to follow the rules and guidance provided on both RBA and ACCC websites:

https://www.accc.gov.au/ https://www.rba.gov.au/

What is my responsibility as a merchant?

If the Merchant surcharges for Transactions, it must:

- Clearly disclose the surcharge to the Cardholder before the Transaction is processed and allow the Cardholder to cancel the Transaction without incurring any cost;
- Ensure any surcharge does not exceed the Merchant's reasonable cost of acceptance as that concept is defined by the Reserve Bank of Australia and by applicable Laws;
- Ensure the surcharge is only charged by the Merchant that provides goods or services to the Cardholder;
- Ensure the surcharge does not differ according to the issuer of the Nominated Card;
- Review the surcharge regularly and at least once every year
- For Refunds, refund any surcharge charged in respect of the Transaction. For partial refunds, the surcharge must be pro-rated; and
- Comply with any Laws, regulations and requirements in the Terminal Guides in respect of surcharging.

When can a new merchant add surcharge? If you are a new merchant and have not yet received any cost of acceptance statement:

- it is advised to wait at least a month and use your first monthly statement.
- However, if you choose to enable surcharging earlier then ensure you are using a rate that is considered realistic and revisit this rate once the cost of acceptance statement is available to you.

How can I enable or update surcharging on an Electronic Terminal?

To set up surcharging, update the surcharge amount or turn off surcharging, the Merchant must:

- contact the Merchant Support on 1800 039 025.
- provide all required details as specified in this merchant guide.
- wait up to 24 hours before the requested changes are effective.

How can I turn off surcharging on an Electronic Terminal?

Contact the Merchant Support on 1800 039 025.

What type of transactions can you add a surcharge to under your Merchant Facility?

You can add a surcharge to the following types of transactions:

- Sales / purchase
- Purchase with Cash Out (on the purchase amount only)
- Purchase with tipping (on the purchase amount only).

How to add surcharging to an Electronic Terminal

1. Review your cost of acceptance statement and identify the cost of acceptance per card scheme you want to apply as a surcharge to, i.e. Eftpos, Mastercard Debit, Mastercard Credit, Visa Debit, and Visa Credit)
2. Decide whether you want to apply surcharge as a fixed amount or as a percentage
3. Call Merchant Support on 1800 039 025 to add these surcharge amounts
4. It can take up to 24 hours before updates are reflected on your Electronic Terminal.

9. Tipping

Tip with transaction allows a specified tip amount to be included as part of the original credit or debit purchase transaction. This functionality allows the cardholder to retain possession of their card at all times and the total value must be verified and authorised by the cardholder at the time of payment. Tip is only available if it has been enabled on the Electronic Terminal otherwise the option will not appear on the display.

Note: The Tip transactions are only available and approved for merchants in specific industries.

10. Cash Out and Purchase with Cash Out

When processing Cash Out and Purchase with Cash Out please note the following:

- Cash Out is not supported on credit cards, contactless, or QR codes.
- Cash Out will not be offered in foreign currencies, i.e. only offered in AUD.
- Cash Out must be authorised online. i.e., no offline transactions.
- Cash Out is only available on (Chip cards)
- Only applicable to certain MCCs
- Maximum amount of Cash Out in a transaction is AUD 500 for Mastercard, AUD 1000 for EFTPOS and AUD 998 for Visa

11. Refunds

Refunds may be processed (as outlined below) if a customer returns goods purchased from you, or for services terminated or cancelled.

Visa and Mastercard

For 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, subject to applicable Laws, 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
- 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, and subject to applicable Laws, 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 as outlined above, and provided that you have adequate supporting documentation proving that the original purchase transaction took place on the original card, subject to applicable Laws, you may offer an alternate form of refund (for example, cash, cheque, instore 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 purchase 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.

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.

If you do so, you may be liable for a chargeback should a cardholder dispute the original purchases transaction, which may result in a debit to your Merchant Account for the relevant "disputed" transaction.

Note: Refund is only available if this transaction type has been enabled on the Electronic Terminal, otherwise the option will not appear on the display. If Refund is not enabled on the Electronic Terminal, please contact ANZ Worldline Payment Solutions on 1800 039 025 for assistance.

Types of refund transactions on Electronic Terminals There are two types of refunds that can processed on the Electronic Terminal:

- A refund transaction, for any purchase that was performed previously
- A reversal transaction, this is when you want to refund the last transaction only.

12. Referenced Refunds

This section of the Merchant Operating Guide applies to:

- all Merchants who have entered into a new Merchant Agreement with Worldline or have been upgraded to the ANZ Worldline Payment Solutions Platform on or after 29th April 2024; and
- all other Merchants for whom Worldline has agreed in writing to enable referenced refunds.

Referenced Refunds are a type of Refund (as defined in the General Conditions) are currently offered on Visa, Mastercard, eftpos and UnionPay International sales transactions only. Referenced Refunds are an optional feature intended to aid in the prevention of fraud through the referencing (matching) of a refund transaction to the original sales (purchase) transaction using the transaction reference number, provided the original sales transaction occurred within the last four (4) months.

Referenced Refunds permit multiple partial refunds or a full refund to the value of the original transaction. Refunds above the original transaction will be declined.

Referenced Refunds will permit refunds in foreign currency using the DCC Service.

For Referenced Refunds use the transaction number and acquirer id located on the terminal receipt to match the exact sales transaction for refund purposes.

Note: Alipay+ and WeChat Pay refunds are always matched to their corresponding original purchase transaction, without any additional or special steps. To process a refund on Alipay+ or WeChat Pay, follow the instructions in the Merchant Operating Guide for the relevant terminal.

Important things to remember when processing a Referenced Refund

- You must always take steps to check the validity of the card and the cardholder's identity.
- You must always obtain the cardholder's consent before issuing the refund and advise them of the amount.
- Advise your customers to retain, and ask that they present, their receipts if requesting a refund. Note: If a customer has a legal right to a refund, you cannot refuse to give this simply because they don't have a receipt if they have other proof of purchase. Please use the standard refund process, not the referenced refund process, in this scenario.
- Referenced Refunds only apply to transactions made in the last four (4) months and should be applied to the same nominated card that was used to make the original transaction. However, you cannot refuse to process a refund simply because it cannot be processed to the same nominated card that was used for the original transaction. Please use the standard refund process, not the referenced refund process, in this scenario.

Referenced Refunds are currently offered on Visa, Mastercard, eftpos and UnionPay International sales transactions only.

- Where the original transaction being refunded was made using the DCC service, the Referenced Refund will always be calculated based on the exchange rate of the original transaction.

- You must always provide a completed transaction receipt for the refund to the cardholder.

Some Refund Scenarios you may encounter

How to process your refund if the original transaction is...	You can perform the refund using:	
	Referenced Refund	Standard Refund
Less than 4 months old and you have the transaction number	✓	✓
Less than 4 months old and was made using DCC (foreign currency)	✓	✓
Older than 4 months with a transaction number		✓
Older than 4 months with *no* transaction number (no receipt)		✓
Has no receipt or transaction number at all		✓
For a transaction where the original card number has changed		✓

Reasons a Referenced Refund may decline and what to do about them.

A Referenced Refund may be declined for several reasons. Please consult the table below for possible causes and suggested actions.

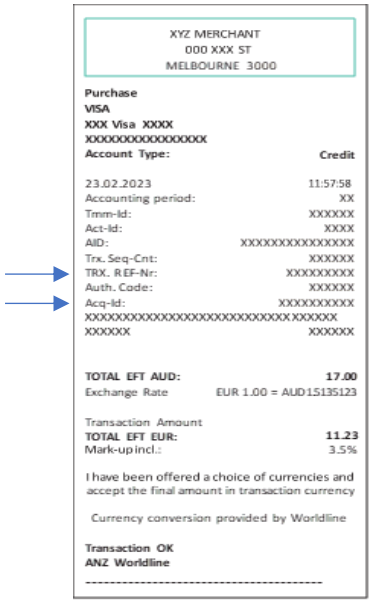
Reasons a Referenced Refund may be declined	Suggested Action
Incorrect acquirer Id or transaction number input	Attempt to process the Referenced Refund again, but using correct information
Refund exceeds the total value of the original transaction	Check the amount to be refunded and ensure it does not exceed the total value of the original transaction. Once this has been confirmed, attempt to process the Referenced Refund again.
Original transaction occurred more than 4 month earlier.	Reprocess using the standard refund processes
Using a different card from the one used for the original transaction	Reprocess using the same card used for the original transaction if possible or perform a standard refund.
Declined by the issuer. E.g: card lost, stolen, or account closed.	Notify the customer, advise them to contact their card issuer and provide the refund in a different way.

If you need help to perform a Referenced Refund, please contact our Merchant Services team on 1800 039 025 for advice.

There are two (2) ways to process a Referenced Refund. Either method may be used as both produce the same refund result.

Note: Be sure to have the acquirer id (Acq-ID) and transaction number (TRX REF-Nr) associated with the original transaction or copy of the original receipt before commencing the Referenced Refund.

(Merchant Copy)


XYZ MERCHANT
000 XXX ST
MELBOURNE 3000

Purchase
VISA
XXX Visa XXXX
XXXXXXXXXXXXXXXX
Account Type: **Credit**

23.02.2023 11:57:58
Accounting period: XX
Tmm-Id: XXXXXX
Act-Id: XXXX
AID: XXXXXXXXXXXXXXXX
Trx. Seq-Cnt: XXXXXX
TRX. REF-Nr: XXXXXXXXX
Auth. Code: XXXXXX
Acq-Id: XXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX XXXXXX

TOTAL EFT AUD: **17.00**
Exchange Rate EUR 1.00 = AUD15135123

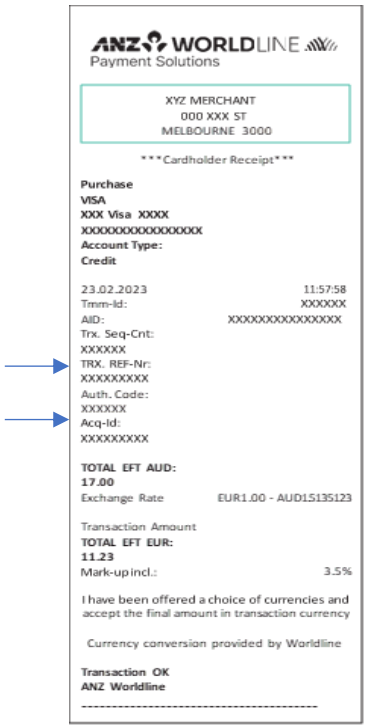
Transaction Amount
TOTAL EFT EUR: **11.23**
Mark-up incl.: 3.5%

I have been offered a choice of currencies and accept the final amount in transaction currency

Currency conversion provided by Worldline

Transaction OK
ANZ Worldline

(Customer Copy)


ANZ WORLDLINE
Payment Solutions

XYZ MERCHANT
000 XXX ST
MELBOURNE 3000

Cardholder Receipt

Purchase
VISA
XXX Visa XXXX
XXXXXXXXXXXXXXXX
Account Type:
Credit

23.02.2023 11:57:58
Tmm-Id: XXXXXX
AID: XXXXXXXXXXXXXXXX
Trx. Seq-Cnt:
XXXXXX
TRX. REF-Nr:
XXXXXXXXX
Auth. Code:
XXXXXX
Acq-Id:
XXXXXXXXXX

TOTAL EFT AUD:
17.00
Exchange Rate EUR1.00 - AUD15135123

Transaction Amount
TOTAL EFT EUR:
11.23
Mark-up incl.: 3.5%

I have been offered a choice of currencies and accept the final amount in transaction currency

Currency conversion provided by Worldline

Transaction OK
ANZ Worldline
---

13. DCC – Dynamic Currency Conversion

What is Dynamic Currency Conversion?

Dynamic Currency Conversion (DCC) allows you to offer a customer the option to pay in their 'home' currency (for Visa and Mastercard transactions only).

This feature provides international Visa and Mastercard cardholders the option of converting Australian currency purchases into their card's billing currency at the time of purchase.

It is important to note that DCC is optional for cardholders, so when you see the DCC screen appear on your Electronic Terminal, you must always ask the cardholder if they would like to pay in their home currency or in Australian Dollars and confirm their acceptance before completing the transaction.

The card schemes (Visa / Mastercard) can mandate that ANZ Worldline deactivate DCC for specific merchants until further notice if this requirement is not met.

The card schemes (Visa / Mastercard) reserve the right to withdraw a merchant's right to offer DCC on transactions.

How does DCC work?

DCC identifies a card's currency and offers the cardholder the option of paying for the goods or services in their card billing currency at the time of purchase.

The exchange rate and price in the cardholder's currency is displayed on the Electronic Terminal.

Accepted currencies for DCC

DCC supports over 40 currencies full list available at anzworldline.com.au/dcc-support

How to process a DCC transaction on your Electronic Terminal

In order to assist a cardholder to make choice as to whether or not to use DCC, you must ensure that:

- If "Choose currency" comes up on the Electronic Terminal, the cardholder must be informed that DCC is optional and has a choice of currencies between the customer's home

  currency and Australian dollars
- The foreign currency transaction amount will contain a X.XX% exchange rate mark-up as displayed on the Electronic Terminal.
- The cardholder has acknowledged that the merchant will conduct the DCC services and accepts the exchange rate and mark-up associated with it.

Note: Exchange rate mark-up is payable to ANZ Worldline Payment Solutions.

Exchange Rates

- The DCC exchange rates will be updated once in 24 hours on all business days at 16:30 p.m. (CET/CEST*)
- During Saturday and Sunday there is no updated rate available, hence the rate from Friday afternoon 16:30 p.m. (CET/CEST) is valid until Monday afternoon 16:30 p.m. (CET/CEST)
- DCC exchange rates can be printed out from the standalone Electronic Terminals once DCC is enabled.. You can find them in the main menu under "Queries".

* CET = Central European Time, CEST = Central European Summer Time.

What are the potential benefits of using DCC?

Benefits to your business include:

- Available at no additional cost
- DCC transactions are settled to your account in Australian dollars
- Customers still have the option to pay in Australian Dollars if they prefer.

Benefits to your customers include:

- Providing cardholders with the ability to view the price and the exchange rate in the cardholder's home currency on the Electronic Terminal at the point of sale.

How will I know a customer's card is eligible for DCC processing?

Once DCC has been enabled, your ANZ Worldline Payment Solutions Terminal has the ability to automatically identify if the card being presented at the point of transaction is eligible for DCC processing. A 'Choose currency' screen will appear once the cardholder has confirmed the original transaction amount and present the card.

EUR = 11.23

AUD = 17.00

Ex.Rate:

1EUR = AUD1.513512335

Mark-up incl : = 3.5%

For example, the 'Ex.Rate: 1.1513512335' shown here is the exchange rate that will be applied to the transaction. The 'EUR' shown refers to the currency the transaction is being converted to, in this case Euro.

The cardholder should now be asked to select the either to pay in AUD or home currency, and accept the exchange rate which includes X.XX% exchange rate mark up as displayed on the Electronic Terminal. Select the home currency (e.g. EUR) if the cardholder accepts DCC or select "AUD" if they prefer to pay in Australia Dollars.

If the customer doesn't want to perform a DCC transaction, they can select "STOP" to cancel the transaction.

Note: exchange rate and exchange rate mark-up displayed here are for illustrative purposes only.

Should I recommend DCC to my customers?

It is the cardholder's choice whether or not DCC is to be applied to their purchase. You should not make any recommendations to the cardholder as they will need to consider their personal financial position and whether DCC is appropriate for them. All you have to do is offer cardholders the choice of having DCC applied to their transaction when prompted by the Electronic Terminal.

DCC offers cardholders the ability to see the value of a transaction in a currency that is familiar to them. The applicable exchange rate is visible to the cardholder and, if they are unhappy with the exchange rate offered, they can choose to pay in Australian dollars.

If a cardholder chooses to pay using DCC, the exchange rate includes an exchange rate mark-up of X.XX% as displayed on the Electronic Terminal. The exchange rate (including the exchange rate mark-up) is clearly displayed to the cardholder on the Electronic Terminal screen before the cardholder opts to convert the transaction.

What are the potential consequences if cardholders initiate a dispute with their card issuer regarding a DCC transaction?

If a transaction was made using DCC Service without the Cardholder's express consent or where you did not fully comply with this condition, you will be liable for the dispute submitted by the Cardholders (and the refund to the Cardholder if the dispute is upheld).

13.1 DCC Rebates

Please also note that if your Agreement provides for a DCC Rebate the following obligations apply:

- The Merchant must comply with all terms and conditions applicable to the DCC Service and the DCC Rebate, including in the General Conditions, the Terminal Guides and any other reasonable instructions given by Worldline on notice in accordance with clause 53 of the General Conditions.
- The Rebate will not be credited to you directly, instead the Rebate will be used to offset fees the Merchant owes to Worldline from time to time.
- Please note: the Merchant must inform all cardholders prior to the Transaction that the Merchant will receive a rebate from Worldline for processing a Transaction using the DCC Service.

14. Mail Order Telephone Order (MOTO)

This function is available only for merchants specifically authorised by ANZ Worldline Payment Solutions.

To process Mail and Telephone Order the Electronic Terminal will request that you identify the 'source' and the 'nature' of the transaction.

Note: You are liable for any disputed transactions. The cardholder may dispute transactions for any reason. To minimise disputes, you should keep the following records of each mail or telephone order

- 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®, Visa® and UnionPay)
- Card number (First 6 and last 4 digits only, e.g. 1234 56XX XXXX 7890)
- Card valid from/to dates
- Authorised dollar amount(s) to be debited
- Contact telephone number
- Details of the goods or services required
- Transaction date.

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

Note: You must retain information about a transaction whether processed manually or electronically for a period of 30 months from the date of the transaction or such other period required by Law or notified by ANZ Worldline Payment Solutions.

15. Pre-Authorisations

Pre-Authorisation
Pre-Authorisation is an optional feature available to eligible merchants. You may enable or disable this feature by contacting the Merchant Support Team on 1800 039 025.

The Pre-Authorisation function reserves funds on a customer's card for a sale transaction to be processed (or cancelled) at a later date for accommodation or vehicle rental. Pre-Authorisation enables a merchant to hold an amount for a validity period (up to 30 days) depending on which card the customer may use.

Pre-Authorisation amounts are not debited until the final payment is processed within the validity period. (Pre-Authorisation Completion).

Pre-Authorisations are available for eligible transactions on Visa, Mastercard, AMEX, JCB and UnionPay International (UPI)cards (Nominated Card Schemes) .

Important Notes about Validity Periods
Nominated Card Schemes set out the *validity period* for holding funds on a customer's card before they must be completed *and* cleared or cancelled.

Validity Periods

Visa:

Pre-Authorisation	Validity Period
Accommodation or vehicle rental	30 calendar days
Motor home or motorcycle rental	10 calendar days

Mastercard:

Pre-Authorisation	Validity Period
Accommodation or vehicle rental	30 calendar days

AMEX and JCB

Pre-Authorisation	Validity Period
Vehicles other than car rental	7 calendar days
Accommodation or car rental exceeding 4 months	For the duration of the stay or rental

UnionPay International (UPI):

Pre-Authorisation	Validity Period
Accommodation or vehicle rental	30 calendar days

Pre-Authorisation transaction types:

Pre-Authorisation
The initial authorisation transaction that reserves funds on a card for a sale to be processed at a later time. The funds are not debited from the cardholder's account until the final payment (pre-authorisation completion) is processed within the validity period.

Pre-Authorisation Completion
A Pre-Authorisation Completion transaction is used to charge the cardholder and remove the reserved/held funds from an earlier Pre-Authorisation transaction (this includes any Pre-Authorisation Adjustments that may have been processed).

Pre-Authorisation Adjustment
A Pre-Authorisation Adjustment transaction is used to increase the value of the original Pre-Authorisation transaction, where the value of the final transaction is higher than the initial reserved amount.

Pre-Authorisation Cancel
A Pre-Authorisation Cancel transaction is used to fully cancel a Pre-Authorisation that is no longer required.

Extending the Pre-Authorisation

If you need to extend the Pre-Authorisation period, you *must*

1. Cancel the original Pre-Authorisation request, and then
2. Submit a new Pre-Authorisation request for the revised amount.

Note: You *must* complete or cancel the Pre-Authorisation at the end of the validity period. Failure to comply may result in chargebacks.

Important things to remember about Pre-Authorisations.

- Always take steps to check the validity of the card and the cardholder's identity.
- Always obtain the express consent of the cardholder and inform them of the amount *before* charging to their card.
- When processing a Pre-Authorisation, the merchant should always apply a genuine estimate of the charges only. and should not include any amount covering potential damage, theft, insurance premium, or tips.
- Merchants will generate an initial receipt on processing Pre-Authorisation request (Pre-Authorisation Receipt). Merchants must retain the Pre-authorisation Receipt as the Pre-authorisation Completion cannot be completed without the *Acquirer ID* and *Transaction Number* details from the receipt.
- Merchants should use the Pre-Authorisation Adjustment transaction to increase (top-up) the amount held if the final amount is higher than the initial request, and before completing the Pre-Authorisation Completion Transaction.
- Cancel or complete all Pre-Authorisations as soon as they are no longer required. You *must not* leave them to expire. This can lead to poor customer experience and scheme fines.
- Cancel the original Pre-Authorisation and submit a new Pre-Authorisation request.

Frequently Asked Questions:

A Pre-Authorisation for AUD 1000 was made using Mastercard, but the actual purchase is for AUD 1200? How do I increase the amount to $1200?

If the final purchase amount is higher than the Pre-Authorisation amount, merchants must perform (Pre-Authorisation Adjustment) for the additional amount. i.e. select Pre-Authorisation Adjustment from the terminal menu, then enter receipt Ref #, and for amount put AUD 200 (for the example above)
Then perform (Pre-Authorisation Completion) for the full amount of AUD 1200.
Based on latest scheme requirements, Tolerance levels have been reduced to zero.

A Pre-Authorisation for AUD 1000 was made using Mastercard, but the actual purchase is only for AUD600? How do I finalise a Pre-Authorisation for a lesser amount?
When processing the (Pre-Authorisation Completion), input the actual amount of (AUD 600) as Pre-Authorisation Completion amount.
The remaining AUD 400 will be released back into the same card used to make the Pre-Authorisation, i.e. the same Mastercard in this example.

Can a Pre-Authorisation be made in a foreign currency using DCC functionality?
No, all Pre-Authorisation transactions can only be processed in AUD currency. DCC cannot be used in any of our Pre-Authorisation transactions (Pre-Authorisation, Pre-Authorisation Completion, Pre-Authorisation Adjustment or Pre-Authorisation Cancel.

Can we use QR code payments to process a Pre-Authorisation Transaction?
No, QR code payments have not been enabled for -Pre-Authorisations

ANZ WORLDLINE
Payment Solutions

anzworldline.com.au

ANZ Worldline Payment Solutions means Worldline Australia Pty Ltd ACN 645 073 034 (“Worldline”), a provider of merchant solutions. Worldline is not an authorised deposit taking institution (ADI) and entry into any agreement with Worldline is neither a deposit nor liability of Australia and New Zealand Banking Group Limited ACN 005 357 522 (“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.