ANZ WORLDLINE
Payment Solutions

ANZ Secure Gateway
ANZ eGate
ANZ ePOS

Merchant Operating Guide

08.22

Contents

1. Welcome

We are pleased 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 on cards you can accept, ways to reduce fraud and what to do if errors or disputes occur. It also contains important information for processing transactions.

Please take time to read this guide thoroughly and ensure that your staff read it too.

This guide covers transactions processed as Card Not Present utilising ANZ Secure Gateway, ANZ eGate or ANZ ePOS products (**eCommerce Products**). If you are processing Card-Present transactions using an EFTPOS terminal not provided by ANZ Worldline Payment Solutions there maybe additional requirements that ANZ Worldline Payment Solutions will inform you of from time to time. If you are using an ANZ Worldline Payment Solutions EFTPOS terminal, please refer to the relevant Operating Guide for your terminal which can be found at anzworldline.com.au/merchant-support.

1.1 MERCHANT AGREEMENT

Your ANZ Worldline Payment Solutions Merchant Agreement contains valuable information and important requirements relating to operating procedures. Instructions in this Merchant Operating Guide form part of the ANZ Worldline Payment Solutions Merchant Agreement 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 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 Nominated Card Scheme may also conduct their own investigations. Your Merchant 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 **ANZ Worldline Payment Solutions General Conditions (General Conditions)** for more details.

Capitalised terms used in this Merchant Operating Guide have the same meaning as in the General Conditions unless otherwise defined.

1.2 IMPORTANT CONTACT DETAILS

ANZ Worldline Payment Solutions
(24 hours a day/7 days a week): 1800 039 025 or merchant@worldline.anz.com

For enquiries directly related to your payment gateway please refer to the contact details provided by your service provider.

1.3 AUTHORISATION

Your payment gateway is designed to automatically seek authorisation from the cardholder's Nominated Card 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.

Note:

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

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

The term 'Authorisation' when used in this Merchant Operating Guide has the meaning outlined above.

1.4 CHANGE OF BUSINESS DETAILS

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

Please visit anzworldline.com.au to complete and submit the respective form or 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
- Ownership
- Bank/branch banking details
- Telephone or fax numbers
- 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.

Note:
If you are using a 3rd party service provider to process your transactions, you are also required to notify them of the changes.

1.5 VOID TRANSACTIONS

Void transactions are transactions that are cancelled by a merchant before the transaction is settled so a cardholder's account is not charged for the transaction. When a transaction is voided it may appear as a pending transaction on the cardholder's account while the process of voiding the transaction is being completed

Note:
A merchant's ability to process void transactions is gateway dependent:

- ANZ Secure Gateway: Available
- ANZ eGate: Available only upon request by merchant
- Non ANZ Gateway: Availability is dependent on gateway offering

Void authorisation is cancelling the funds a merchant authorised for a cardholders purchase. After an authorisation transaction has been cancelled/voided, the merchant cannot capture any funds associated with that transaction and authorisation hold on the cardholders account will be removed.

Void transactions are different from refunds. Voiding a transaction cancels the original authorisation before the cardholder is charged for the goods or service. A void transaction does not appear on the cardholder's account statement as a processed transaction. Whereas, refunds are issued after a transaction has settled and the cardholder has paid for the good or service.

2. Cards You Can Accept

Credit Cards and Debit Cards

Cardholders can use credit cards or debit cards (Visa, Mastercard and, where it is enabled, UnionPay) to access their card accounts.

Note:
Not all ANZ Worldline Payment Solutions eCommerce Solutions support UnionPay.

Charge Cards

Processing charge cards is essentially the same as processing credit card transactions. However, to accept charge cards, you must have an agreement with the charge card Issuer (e.g. Diners Club, American Express and JCB).

3. Fraud Minimisation

Fraud may be a problem for 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 payment is found to be fraudulent, it may be charged back to you, possibly leaving your business out of pocket. High fraud and Chargeback levels can also put the future of your Merchant Facility in jeopardy as it can result in your Merchant Agreement being terminated and/or attract penalties from the Nominated Card Schemes (such as Visa and Mastercard).

For more information, please refer to the General Conditions.

3.1 FRAUD MINIMISATION FOR CARD PAYMENTS

Mail, Telephone and Internet Orders

Any credit or debit card transaction where the card and/or cardholder is not present poses a higher risk to your business. Being vigilant about unusual spending or behavior 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 (i.e. it could be fraud).

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.

Records of each mail, telephone and Internet order 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 (such as Mastercard or Visa)
- Card number (first six and last four 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

In addition to this, you may also want to consider doing the following once the order has been placed:

- Telephone the customer to confirm the order
- Obtain authorisation for all orders from the customer
- Verify the delivery address and order details
- Check the delivery details to verify the name, address and telephone number

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

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 or 4 digits on the signature panel on the back of the card. The Security Code must never be recorded for future use.

As of 1 April 2012, all online payment facilities must also have the security code/CVV2 field enabled on their web payment page.

Common indicators of Fraud

The below are potential indicators of fraudulent activity, however these indicators may not always represent cases 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 telegraphic transfer, or other means. 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.
- 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 potential 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 (e.g Mobile Phones).
- Refund Requests: Specifically when orders are cancelled and refunds are requested via telegraphic 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.

Best Practice Advice

- 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.
- The name of the Card Issuing Bank and the country the card was issued in.
- Capture the cardholder's Security Code/CVV2 or CVC2 represented by the last 3 digits on the back of the card, but do not retain this information once the transaction has been processed.
- Call customer for follow up after the transaction. This will establish the contact details they have provided are valid.
- For purchases by a business, 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.
- If requested by your customer to do so, never make a payment in excess of the sale value with the intention of transferring the excess amount to a third party.
- Always follow the instructions contained in the "Refund" section of your Terminal Guide when processing a refund.
- 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 accept payments via your website and use a 3rd party Gateway provider, 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.
- 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.

3.2 3D SECURE – ONLINE AUTHENTICATION TOOL

'Visa Secure, 'Mastercard Identity check and Mastercard SecureCode' are collectively referred to as 3D Secure (3DS). These are online, real-time security tools for merchants who trade online to validate that a cardholder is the owner of a specific card number. This will help protect merchants against certain fraudulent Chargeback cases.

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 Visa Secure, Mastercard Identity Check and Mastercard SecureCode window will appear. The cardholder will then be prompted to complete verification. The method of verification may vary depending on the cardholders bank.

Following verification of the cardholder by their Bank, the window disappears and the cardholder is returned to the checkout screen. If the cardholder is not verified, the transaction will be declined.

Merchants utilising 3DS are protected from receiving certain fraud-related Chargebacks.

For further information about Visa Secure, Mastercard Identity Check and Mastercard SecureCode or to ensure your 3rd party gateway supports 3DS via ANZ Worldline Payment Solutions, please contact ANZ Worldline Payment Solutions on 1800 039 025.

Note:
If you are operating via a 3rd party gateway provider, it is your responsibility to ensure that the correct risk management rules are applied to your payment facility.

3.3 AMERICAN EXPRESS SAFEKEY

American Express (**AMEX**) SafeKey is an authentication tool provided by AMEX that operates based on the 3D Secure protocol. AMEX SafeKey is intended to provide participating AMEX merchants a layer of fraud protection for online AMEX transactions by verifying the cardholder's online identity. This may help merchants reduce fraudulent AMEX chargeback cases and provide a

more secure and better online shopping experience for both merchant and AMEX cardholders.

For further information about AMEX SafeKey or to ensure your 3rd party gateway supports AMEX SafeKey via ANZ Worldline Payment Solutions, please contact ANZ Worldline Payment Solutions on 1800 039 025

3.4 THIRD PARTY TRANSACTIONS

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

Potential impacts to your business include:

- You may be in breach of Scheme (Visa & Mastercard) rules and be open to possible fines
- You may be unwillingly committing, and becoming involved in, fraud
- Your Merchant facility may be terminated.

3.5 CAPTCHA

Captcha is a means of distinguishing humans from malicious bots on the internet. Bots are automated programs designed to simulate human interactions with a website, with many bots being designed with malicious intent. Captcha utilises a challenge / response approach that humans can pass, but computer bots cannot.

ANZ Worldline Payment Solutions recommends the use of Captcha for accepting payments using a website.

4. Handling cardholder information securely & PCI DSS

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

Businesses store credit or debit 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 recommends that card data is never stored on your systems.

You must ensure all cardholder data and Transaction Records are received, processed and stored in compliance with the Payment Card Industry Data Security Standard (PCI DSS).

ANZ Worldline Payment Solutions suggests using a secure eCommerce solution, to capture, process and store card details. Solution examples include hosted payment pages or iframes where the page capturing the data is served by the PCI DSS compliant payment gateway. This will minimise the risk of card data being stolen from your environment.

PCI DSS and Data Storage Requirements

PCI DSS is a set of standards implemented by the Nominated Card Schemes, to help manage the risk to merchants from data breaches or hacker access. The standards apply to all merchants who capture, process and store credit or debit card data in any format, have access to card details, or have systems which enable internet access to their company/business 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 activities.
- Your business may experience improved patronage due to customers' confidence in the secure handling of their 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 – It is recommended that cardholder data is not stored by your business and if you do choose to store this information, it must be stored securely.

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.

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 further information relating to these programs, please visit the following websites:

- Visa
  - https://www.visa.com.au/partner-with-us/pci-dss-compliance-information.html
  - https://www.visa.com.au/support/small-business/security-compliance.html#1
- Mastercard
  - https://www.mastercard.com.au/en-au/merchants/safety-security/security-recommendations/site-data-protection-PCI.html
  - https://www.mastercard.com.au/en-au/merchants/safety-security/security-recommendations/merchants-need-to-know.html

It is vital to protect your customers and your business against misuse of credit and 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).

ANZ Worldline Payment Solutions may contact merchants and request that they be PCI DSS compliant based on their volumes or risk profile or if they have had a data compromise event.

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

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 4 different SAQs, covering a variety of payment processing environments, available to download from the PCI SSC website at:

https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

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://www.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 and forms part of your compliance with PCI DSS.

An external vulnerability scan is only one of the many tools that 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 such vulnerabilities so they can be corrected.

Securing Transaction Records

In general, cardholder data must not be stored unless it is strictly for use within the business and absolutely necessary. However, you may be required to store cardholder data and Transaction Records. If so, it is your responsibility to ensure all paper and electronic records containing cardholder data are secured (e.g. locked filing cabinet or encrypted in a secure environment).

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 that you process transactions with security codes (CVV2/CVC2), but do not store these codes after they have been authorised.
- Use a payment gateway to keep cardholder data storage to a minimum, and only what is necessary for business or legal needs.
- Once a transaction is processed, obscure all

digits except the first 6 and last 4 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 to your customer's card details. Do not have generic users and delete any defaults.
- Avoid storing cardholder data on PC's, laptops or mobile phones.
- Do not store your customers' card details online or unencrypted on your computer.
- Securely dispose of cardholder data as soon as its use has expired. PCI DSS recommends cross 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.
- Always patch your systems and website to the most recent software versions.

Under no circumstances should sensitive information be stored; this information includes security codes (CVV2, CVC2), PIN or magnetic stripe data.

The following sources provide guidance on card data storage:

The **General Conditions** – see Section 14 'Information collection, storage and disclosure'.

For more information, visit the PCI Security Standards Council website at https://www.pcisecuritystandards.org/index.shtml

In the event of a data compromise, immediately contact ANZ Worldline Payment Solutions for support.

5. Chargebacks

A Chargeback is the term used for debiting a merchant's bank account with the amount of a transaction that had previously been credited. Chargebacks can have a financial impact on your business. 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 (Nominated Card Schemes-issued) card sale where you have failed to follow the Bank's procedures or Nominated Card Scheme rules as stated in this Merchant Operating Guide or in the General Conditions. 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.

Note:
You must securely 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.

A cardholder can generally raise a Dispute/ Chargeback with their bank (issuing bank) up to 120 or 240 days (dependent on the reason code and Nominated Card Scheme) from the date of the transaction but in some instances can be up to a maximum of 540 days. The cardholder can raise a dispute for many reasons, however, the most common reasons for Chargebacks on Card Not Present transactions are:

- Processing errors
- Unauthorised use of a card
- Unauthorised transactions
- Invalid card account number
- Incorrect transaction amount
- Expired card
- Transactions performed on a lost or stolen card
- Failing to respond to a Transaction Evidence Request letter
- 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 for further details.

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

6. Refunds

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**).

Note:
If you require assistance processing a refund via an alternate method, please contact ANZ Worldline Payment Solutions on 1800 039 025 (24 hours a day, 7 days a week).

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.

Note:
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.

7. Settlement

ANZ Worldline Payment Solutions offers same day settlement, every day.

For ANZ business account holders with:

- ANZ Secure Gateway*, the funds are available on the same day for online transactions processed and settled before 5:30pm (AEST);
- ANZ eGate*, the funds are available on the same day for online transactions processed and settled before 6:30pm (AEST); and
- ANZ ePOS, the same day settlement cut off times are dependent on the third party gateway being used.

For non-ANZ business account holders, ANZ Worldline Payment Solutions transfers the funds to the merchant's bank on the following business day and the availability of the funds will be determined by the merchant's bank. For transactions processed offline or via Paper Merchant Vouchers, these settlement times do not apply.

American Express, Diners Club and JCB will credit your bank account separately. Please check directly with these third parties for when funds are available as times may vary.

*Please note that settlement of transactions is reliant on the transaction information being provided by the gateway provider to ANZ Worldline Payment Solutions. There may be instances where a failure occurs that results in transaction information not being submitted to ANZ Worldline Payment Solutions in the required timeframe. In this instance and in a scenario where ANZ Worldline Payment Solutions receives unprecedented transaction volumes in a single day, this could result in funds for certain transactions not being available on the same day, and instead these transactions will be credited as part of the following days settlement.

8. Pre-Authorisations

A merchant operating certain types of businesses, such as hotels or car rentals, can be approved to process a Pre-Authorisation Transaction.

A Pre-Authorisation is used to place a hold on the cardholders' funds to the value of the transaction to be processed at a later time, for example, a hotel may reserve funds to pay the final bill upon checkout. These transactions can only be performed on credit card accounts.

The term Pre-Authorisation used across this Merchant Operating Guide will have the same meaning unless otherwise defined.

Some examples are listed below to assist in estimating your Pre-Authorisation amount:

Example 1: A hotel may estimate transaction amounts based on:

- Cardholder's intended length of stay at check-in time
- Room rate
- Applicable tax
- Service charge rates
- Other allowable charges (e.g. mini-bar and telephone calls).

Example 2: A Car Rental Company may estimate transaction amounts based on:

- Cardholder's intended car rental period
- Rental rate
- Applicable tax
- Mileage rates
- Other allowable charges (e.g. petrol and extra mileage).

8.1 REQUIREMENTS FOR PROCESSING PRE-AUTHORISATIONS

Visa and Mastercard have defined global requirements in regards to the processing of Pre-Authorisations. These requirements are in place to improve the experience for both the cardholder and merchant when using the Pre-Authorisation functionality.

When processing Pre-Authorisation transactions, you must:

- Only process a Pre-Authorisation where the final amount of a transaction is not known.
- Cancel or complete all Pre-Authorisations. You cannot leave a Pre-Authorisation to expire.
- Where the authorisation is required for longer than the approved validity period, request for an extension of the authorisation (refer to your gateway provider for details on how to request for an extension). Refer below for further information about validity periods.
- To avoid confusion with the cardholder, you will need to disclose to the cardholder when a Pre-Authorisation is performed.

8.2 PRE-AUTHORISATION VALIDITY PERIODS

Mastercard:

- Mastercard Pre-Authorisations are valid for 30 days unless the authorisation has been completed or cancelled
- Refer to section 8.3 Pre-Authorisation Features for split shipment Pre-Authorisation validity periods

Visa:

- Visa Pre-Authorisation validity is based on business type which is listed below:

Business Type	Validity period
Hotels, vehicle rental, cruise lines	31 days
Other rental businesses (e.g. boat rental, trailer park, bike rental, transportation, passenger railways, bus lines)	7 days
Amusement Parks Restaurants & Bars Taxis – Card Not Present transactions only	Same Day as authorisation

- Refer to section 8.3 Pre-Authorisation Features for Split shipment Pre-Authorisation validity periods

8.3 PRE-AUTHORISATION FEATURES

Reauthorisation

You can initiate a reauthorisation when the completion of the original order extends beyond the authorisation validity limit. Common scenarios for reauthorisation include: extended hotel stays, delayed shipments etc. You can extend the authorisation for up to 120 days.

Incremental

An open Pre-Authorisation can be increased if the initial authorisation amount was insufficient. Completing an incremental authorisation does not replace the original transaction – it is in addition to any previously authorised amount. An incremental authorisation will not extend the validity of the original authorisation.

Split Shipment

Split shipment is only available for Visa and MasterCard transactions as specified below. A Merchant may obtain a single Authorization and submit multiple clearing records only in the following circumstances:

1) Where the Merchant is an airline or a cruise line.

2) Where the Merchant is a card-not-present merchant that ships goods, and all of the following circumstances apply:

- The purpose is to support a split shipment of goods;
- The transaction receipts associated with each shipment contain:
  - the same payment credential and expiration date;
  - the same merchant outlet name;
- Prior to purchase the Merchant discloses to the Cardholder the possibility of multiple shipments on its website and/or application or in writing;
- With each shipment, the Merchant notifies the Cardholder of the transaction amount of the shipment;
- The transaction is not completed with a Visa commercial card enrolled in Authorization and settlement match; and
- Split shipment Authorisation response is valid no later than 7 calendar days from date on which the first Authorisation request received an approval response.

3) Where split shipment is approved by ANZ Worldline Payment Solutions in relation to the relevant gateway and merchant.

4) Where the Merchant is not using split shipments in contravention of or to circumvent the operation of any Nominated Card Scheme rules.

A merchant's ability to process split shipment transactions is dependent on whether their gateway can provide split shipment. A merchant will need to request for split shipment functionality from their gateway provider for it to be enabled.

Partial cancel

An open Pre-Authorisation amount can be partially reduced. This may be required where the full amount of funds being held is no longer required. The cancellation will be sent immediately and the funds will be available to the cardholder as soon as it is processed by their bank.

Cancel

As soon as you are aware that you will not be completing the amount held for Pre-Authorisation, you must cancel the Pre-Authorisation. You can use the cancel feature to return the full amount to the customer's card. The cancellation will be sent immediately and the funds will be available to the cardholder as soon as it is processed by their bank.

Merchants that use Pre-Authorisations and the above features must utilise appropriate data values for the different transaction types. You should discuss these requirements with your gateway provider to ensure you are meeting these requirements.

Nominated Card Scheme rules require all Pre-Authorisations which are not completed to be cancelled within the time periods outlined at section 8.2 above.

9. Storing Card Data for Future Payments

Merchants commonly obtain customers card data to process transactions at a later date as agreed with the cardholder. There are a number of requirements as below that must be met when completing such transactions.

9.1 REQUIREMENTS FOR STORING CARD DATA FOR FUTURE USE

It is required that you receive consent from your customer before storing their payment data. To request the initial storage of credentials you must obtain the cardholder's consent informing them as per below:

- How the cardholder will be informed of the changes to the consent agreement;
- The expiration date of the consent agreement;
- How the Stored Credentials will be used; and
- A truncated version of the stored card number

If you are going to use the stored card details to initiate transactions, you must also provide the cardholder with:

- Your cancellation and refund policy
- Your full postal address, including country and telephone number
- The amount that will be charged, or details of how it will be calculated
- Any additional fees or surcharges
- The transaction frequency or the event that will initiate the transaction

Merchants that offer cardholders the opportunity to store their payment data on file must send specific data when processing these transactions. You should discuss these requirements with your gateway provider to ensure you are meeting these requirements.

9.2 FEATURES AVAILABLE WHEN STORING CARD DATA FOR FUTURE USE

Delayed Charges

An additional transaction can be processed to a cardholder within 90 days after the original services have been rendered and original payment has been processed. This is only available for hotels and businesses that provide vehicle or other rentals.

No Show

As per your cancellation policy, you can perform a No Show penalty charge if the cardholders use a Visa card to process a guaranteed reservation. A guaranteed reservation ensures that the reservation will be honored and held until the cardholder arrives. This is only available for hotels and businesses that provide vehicle or other rentals. This feature is not available for other Nominated Card Schemes other than Visa.

Account verification using $0

You can process a Pre-Authorisation or transaction for $0.00 to confirm that a card is valid to setup a recurring payment. This feature of account verification can be used when a card number needs to be validated prior to setting up a recurring payment.

Card Data on File for Recurring and Installment payments

You can process recurring and/or installment payment (not more than a year's apart) on behalf of the cardholder. These can only be performed once you have received consent from the cardholder to do so.

9.3 TOKENISATION – ONLINE SECURITY TOOL

A Scheme/Network Tokenisation (Tokenisation), refers to an online security tool that replaces a cardholder's card number with an algorithmically generated number called a token.

The token is merchant specific and the same token is generated each time the merchant processes a transaction for that card. Replacing the card number with a token end to end in the payments flow, is intended to provide an additional layer of security to a cardholder's data and safeguard against a data breach.

Tokenisation may also elevate the cardholder's experience in other ways. For example, Tokenisation digitises the physical card asset as card art and facilitates better card lifecycle management where card details are automatically

updated, allowing payments and services to remain up to date.

A merchant's ability to process Tokenisation is dependent on whether their gateway provider can provide Tokenisastion. If so, the merchant will need to request their gateway provider to enable Tokenisation.

A merchant will also need to enroll for Tokenisation with the relevant Nominated Card Schemes such as Visa/MasterCard. A merchant's implementation of Tokenisation may be subject to delay depending on the enrolment process for Tokenisation, as Nominated Card Schemes may complete the enrolment process at different times.

10. Surcharging

The Reserve Bank of Australia's Standard No 3 of 2016 provides regulation for merchants who choose to apply a surcharge on card payments.

The regulation defines how much a merchant can surcharge and prohibits merchants from applying a surcharge that is greater than their cost of accepting that card type.

Further information is available at anzworldline.com.au/merchant-support-regulations

It is your decision whether you choose to surcharge for card payments.

If you do not surcharge for card payments your business is not affected by the regulation, unless you decide to surcharge in the future.

When applying a surcharge to a transaction, the surcharge amount must comply with the following:

- Be limited to the "reasonable cost of acceptance" as that concept is defined by the Reserve Bank of Australia and by applicable laws or regulations.
- Be clearly disclosed to the cardholder before the completion of the transaction. The cardholder must be given the opportunity to cancel without penalty after the surcharge is disclosed.
- Be charged only by the merchant that provides the goods or services to the cardholder. The merchant must not permit a third party to charge a cardholder a separate or additional amount in respect of the cost of acceptance of the card, but the Merchant may include third-party costs relevant to accepting a card as part of the surcharge.
- Not differ according to Issuer.
- Be assessed only on the final total amount charged for the goods or services, after any discount or rebate from the Merchant has been applied.
- Be added to the Transaction amount and not collected separately.

A Merchant that applies a surcharge must do all of the following:

- Inform the cardholder that a surcharge is applied.
- Inform the cardholder of the surcharge amount or rate.
- Not describe the surcharge as, or inform the cardholder that the surcharge is, applied by the scheme or a financial institution.
- Include notices, signs, or decals disclosing that the Merchant applies a surcharge. Such notices, signs, or decals must be in a conspicuous location or locations at the Merchant's physical point of sale, or, in the absence of a physical point of sale, prominently during an Electronic Commerce Transaction or communicated clearly in a telephone order so as it can be reasonably assured that all cardholders will be aware of the charge.
- Clearly display or communicate the surcharge disclosure in the Transaction environment or process. The disclosure must be of as high a contrast as any other signs or decals displayed.

A Merchant must clearly and prominently disclose any surcharge that will be applied.

The disclosure must include both:

- The exact amount or percentage of the surcharge.
- A statement that the surcharge is being applied by the Merchant.

For an Electronic Commerce Transaction, a Mail/Phone Order Transaction, and an Unattended Transaction, the cardholder must be provided the opportunity to cancel the Transaction subsequent to the surcharge disclosure.

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 SAs market-leading payments technology and future innovations. ANZ Worldline Payment Solutions commenced operations on the 1st April, 2022.

Pairing Worldline SAs 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**"), 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.

Item No. AW2038 08.2022 WZ123081 200.0025.02_AUS_EN/08.22