ANZ WORLDLINE
Payment Solutions

Worldline Global Online Pay

Merchant Operating Guide

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 guide covers operational and Nominated Card Scheme requirements you need to follow to process eCommerce Transactions using the Worldline Global Online Pay.

Merchants can also refer to the ANZ Worldline Merchant Portal User Guide within the Merchant Portal. This guide will provide you with information on how to use and navigate through the Merchant Portal (including information about payment links).

Please take time to read both guides thoroughly and please ensure that anyone in your business who operates your Worldline Global Online Pay reads this guide too.

1.1 MERCHANT AGREEMENT

Please read this Merchant Operating Guide with your ANZ Worldline Payment Solutions Agreement, as your Merchant Agreement also contains important information relating to the operating procedures of Worldline Global Online Pay.

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**)

Please ensure that you follow the security checks and procedures in this guide to assist in identifying and minimising fraudulent, invalid or unauthorised 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 Agreement outlines the circumstances in which you will be liable for such transactions. If it is found that you have processed invalid or unauthorised 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 or anzecommercesupport@worldline.anz.com

1.3 AUTHORISATION

Worldline Global Online Pay 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 any merchant from chargebacks.
- Authorisation Declined: Where an authorisation is declined, please seek an alternative method of payment.

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 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 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.

1.5 WORLDLINE GLOBAL ONLINE PAY SUPPORT SITE

The Worldline Global Online Pay Support Site is a website that provides information about Worldline Global Online Pay and documentation to support your integration set up into Worldline Global Online Pay.

The content on the Worldline Global Online Pay Support Site is provided for customers in several different countries. This means that, in some cases, European terminology (e.g. VAT or value added tax), currency (Euros) or concepts may be used. These are examples only.

The Worldline Global Online Pay Support Site is also intended to focus on gateway/acceptance requirements and does not include all acquiring requirements. When reading the Worldline Global Online Pay Support Site, keep in mind that for your Merchant Facility, ANZ Worldline Payments Solutions is both the acquirer and provides the gateway/acceptance services. For this reason and due to the Worldline Global Online Pay Support Site's global audience, we ask you to note that not all content on the site will be relevant to your use of Worldline Global Online Pay here in Australia.

Please refer to this Merchant Operating Guides, instruction manuals and your Agreement for more detailed information applicable to your Worldline Global Online Pay Merchant Facility.

Please take time to read this material thoroughly and please ensure that anyone in your business who operates your Worldline Global Online Pay reads this guide too.

For technical guidance and support please refer to: https://anzworldline.com.au/wlop-support

2. Core Features

2.1 PLUGINS AND INTEGRATION OPTIONS

ANZ Worldline Payment Solutions has enabled a wide range of plugins and integration methods. Please refer to the Worldline Global Online Pay Support Site for our current available plugins and integration methods, their features, and their compatibility with your preferred e-commerce platform.

A merchant can connect their e-Commerce platform with Worldline Global Online Pay through a Plugin or various API integration methods.

A Plugin, also commonly known as a Shopping Cart Plugin is an out-of-the box solution that allows you to process payment quickly via a simple integration.

Merchants can use these plugins to streamline the integration process and leverage Worldline Global Online Pay within their preferred e-commerce environment. You will need to sign up and form a separate agreement with the plugin provider.

To integrate your e-Commerce environment into our supported Worldline Global Online Pay plugins, you will need to utilise your PSP ID and API credentials (API Key and API Secret Key) which can be generated from your Merchant Portal. Please ensure your API credentials are not disclosed to unauthorised parties, and only disclosed to parties such as your developer who will require access to create and manage your integration. Providing someone with your API credentials and PSP ID enables them to link your Merchant facility to other plugins and shopping carts.

For Merchants that have a custom-built website, ANZ Worldline Payment Solutions can offer additional API integrations as follows:

- Hosted Checkout Page
- Hosted Tokenisation Page
- Mobile/Client Integration
- API integration. (Server-to- Server)

These options provide you with the flexibility to integrate Worldline Global Online Pay services into a custom-built website. For more information about these integration methods please refer to the Integration page within the Worldline Global Online Pay Support Site.

Please be aware that the Merchant is solely responsible for the integration, installation, operation, maintenance and security of its connection to Worldline Global Online Pay.

2.2 PAYMENT LINKS

Payment Links, also known as Pay By Link, is a feature offered by the Worldline Global Online Pay that allows Merchants to collect payments through a link sent via email. This feature provides a convenient and secure way for Merchants to request payments from their customers.

Here is some more information about how it works:

Merchants can create a Payment Link that can be sent to their customers via email. The link will direct the customer to a secure payment page where they can enter their payment information and complete the transaction.

The Merchant Portal allows Merchants to create and manage Payment Link transactions. Merchants can customise the Payment Link to include specific amounts or product details, and they can track the status of each transaction.

For more information, please refer to the Merchant Portal Operating Guide found within the Merchant Portal.

3. Accepting Payments

3.1 CREDIT CARDS AND DEBIT CARDS

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

3.2 ALTERNATIVE PAYMENT METHODS

WeChat and Alipay+ are alternative payment methods (**Alternative Payment Methods**) that can be enabled on the Worldline Global Online Pay.

If enabled, your customer can also pay using digital wallets such as WeChat Pay, Alipay+, and the other digital wallets enabled through Alipay+ if available on Worldline Global Online Pay.

More information regarding WeChat Pay and Alipay+ is located in section 4.53 below.

3.3 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, JCB) and wallets (e.g. PayPal, Google Pay and Apple Pay).

To ensure a seamless integration and efficient processing of payment methods such as American Express, Diners, JCB, and others (PayPal, Google Pay), Merchants must establish a separate agreement with each provider. Additionally, it is crucial for Merchants to provide the correct contract number, merchant ID or payer ID associated with these payment methods. Failure to do so may result in delays in enabling these payment options in Worldline Global Online Pay.

Please note that ANZ Worldline Payment Solutions does not act on behalf of or represent any of the payment method providers listed and will not be a party any agreement you may choose to enter into with a payment method provider.

Any information provided is general in nature and does not take into account your needs, financial circumstances or objectives. You should consider whether it is appropriate for you. ANZ Worldline Payment Solutions does not provide any financial, investment, legal or taxation advice.

4. Transactions

4.1 ACCEPT PAYMENTS

Merchants can make a payment via the Merchant Portal and/or through their shopping cart plugins that are integrated into Worldline Global Online Pay.

4.2 CANCEL A PAYMENT

Merchants can cancel a payment before it is settled so a cardholder's account is not charged for the transaction. When a transaction is cancelled it may appear as a pending transaction on the cardholder's account while the process of cancelling the transaction is being completed

After an authorisation transaction has been cancelled, the Merchant cannot capture any funds associated with that Transaction and authorisation hold on the cardholders account will be removed.

Cancelling transactions is different from refunds. Cancelling a transaction reverses the original authorisation before the cardholder is charged for the goods or services. A cancelled 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.

4.3 PRE-AUTHORISATION

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

4.31 PRE-AUTHORISATION VALIDITY PERIODS

Mastercard

- Mastercard Pre-Authorisations are valid for 30 days unless the authorisation has been completed or cancelled
- Refer to section 4.32 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 4.32 Pre- Authorisation Features for Split shipment Pre-Authorisation validity period.

4.32 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.

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

A merchant will need to request for split shipment functionality 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 ANZ Worldline Payment Solutions 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 4.32 above

4.4 CHARGEBACKS

A Chargeback is the term used for debiting a merchant for the amount of a transaction that had previously been credited.

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.

Note: You must securely retain information about a transaction whether processed manually or electronically for a period of 13 months from the date of the transaction or such other period required by 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.

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. 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.

The cardholder can raise a dispute for many reasons, however, the most common reasons for Chargebacks on eCommerce 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 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).

4.5 REFUNDS

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

4.51 VISA AND MASTERCARD

For any goods purchased with a Visa and Mastercard 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).

4.52 OTHER CARD SCHEMES

Unionpay

To process a UnionPay refund a merchant must comply to the following requirements for a refund transaction.

- A Merchant shall comply with requirements for refund transactions, conduct the refund and return the amount to the cardholder's account used for the original transaction;
- A Merchant shall provide the refund service for UnionPay Cardholders with the same service level as that for cash payments;
- A Merchant can process multiple refunds provided the refund amount shall not exceed the original transaction amount;

- A Merchant shall post a notice in a prominent place if the Merchant does not provide UnionPay Card Refund services, or only uses goods of equivalent value for replacement instead of providing Refunds.

Other Schemes or Alternative Payment Methods

For any goods purchased with a card belonging to schemes other than the Visa Mastercard or, UnionPay 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.

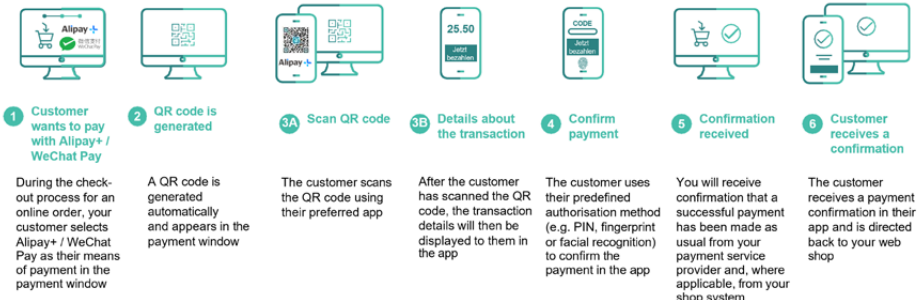
Note: If a refund transaction is performed on an international card, please advise the cardholder that the refund amount displayed on their statement may vary from the purchase amount due to the changes in currency exchange rates.

To process an Alipay+ / WeChat Pay refund a Merchant must comply to the following requirements for a refund transaction.

- The Merchant must communicate to customers its refund and after-sale service policies
- If a customer requests an Alipay+ / WeChat Pay refund under the Merchant's refund or after-sale service policies, and any applicable laws – such a refund must be granted to the customer through Alipay+ / WeChat Pay, respectively
- The Merchant must process this refund within 365 days from the date of the original Transaction
- A Merchant shall comply with requirements for refund transactions, conduct the refund and return the amount to the cardholder's Alipay+ / WeChat Pay wallet, respectively, that was used for the original transaction

4.53 ALIPAY+ AND WECHAT PAY

The diagram below illustrates the payment experience when your customer pays with an Alipay, WeChat Pay or a digital wallet enabled by Alipay+:



Note that the QR code is interoperable, this means that the one QR code for a transaction can be scanned by any of the supported digital wallets.

5. Acquiring Features

5.1 SETTLEMENT

ANZ Worldline Payment Solutions offers same day settlement, every day to anANZ business transaction account processing major card transactions. This is subject to the terms of your Agreement, which allow settlement to be deferred in several situations. Please refer to your Agreement for details.

For settlement to an ANZ business transaction account the funds are available on the same day for online transactions processed and settled before 9:30pm (AEST) unless deferred under the Agreement.

For settlement a non-ANZ business account, ANZ Worldline Payment Solutions generally 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, unless deferred under the Agreement.

American Express, Diners Club and JCB will settle and credit your bank account separately.

Please check directly with these third parties for when funds are available as times may vary.

The proceeds from any Alipay+ or WeChat Pay transactions will generally settle on two Business Days' following the date the sales Transaction was originally processed, unless deferred further under the Agreement.

5.2 SURCHARGING

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.

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.

A Merchant is responsible for determining the surcharge amounts based on the obligations under the RBA Standard. ANZ Worldline Payment Solutions can enable and configure the surcharge amount, as advised by the Merchant in the Worldline Global Online Pay.

It is important to note that ANZ Worldline Payment Solutions does not assume any liability to ensure compliance with RBA rules and regulations regarding the surcharge amounts, nor does it validate the surcharge processed via API you have used to integrate Worldline Global Online Pay.

When applying a surcharge to a transaction, and in addition to any other compliance requirements mentioned in the General Conditions, the surcharge amount must comply with the following:

- 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.

In all cases, including eCommerce Transactions, the cardholder must be provided the opportunity to cancel the Transaction after the surcharge disclosure.

5.3 DYNAMIC CURRENCY CONVERSION - DCC

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.

DCC is optional for cardholders. No default option or pre-selection is allowed.

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

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:

- Offering transparency to customers because the price and exchange rate are displayed on the Payment details page at the time of the check out.
- Customers do not need to worry about calculating the difference between the DCC rate and non-DCC rate for their transactions.

Accepted Currencies For DCC

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

DCC Transactions on Worldline Global Online Pay

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 the check out. The exchange rate and price in the cardholder's currency is displayed on the Payment details page.

To assist a cardholder to make decision regarding whether to use DCC, the following information and disclaimer will be displayed:

- The foreign currency transaction amount includes a X.XX% exchange rate mark-up.
- By choosing to pay in your local currency, you accept the exchange rate and the amount in the selected currency.

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)

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

Frequently Asked Questions

How will a customer know whether the card is eligible for DCC processing?

Once DCC has been enabled, your Worldline Global Online Pay gateway can automatically identify if the card used at the time of the check out is eligible for DCC processing. 'Select Currency' will appear once the card number is entered:

Example:

Select Currency

- **Pay $29.80 AUD**
- **Pay €18.71 EUR**

Exchange Rate 1.00 AUD = 0.62778704 EUR Inclusive of Mark-up = 3.5%

'Exchange Rate 1.00 AUD=0.62778704 EUR' shown here is the exchange rate that will be applied to the transaction. 'EUR' refers to the currency the transaction is being converted to, in this case Euro. The cardholder should now be asked to select either to pay in AUD or home currency and accept the exchange rate which includes a 3.5% exchange rate mark-up. Select the home currency (e.g., EUR) if the cardholder accepts DCC or select "AUD" if they prefer to use AUD.

If the customer does not want to perform a DCC transaction, they can select "Cancel" to cancel the transaction.

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

Should I recommend DCC to my customers?

It is the cardholder's choice whether 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.

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 displayed on the Payment details page includes an exchange rate mark-up of X. XX%. The exchange rate (including the exchange rate mark-up) is clearly displayed to the cardholder on the Payment details page before the cardholder opts to convert the transaction.

What are the additional requirements for processing a refund transaction?

Refund transactions must always be processed in the currency of the original transaction.

The original transaction must be selected to ensure the same exchange rate (including mark-up) is applied to the refund to avoid exchange rate differences.

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).

6. Fraud Minimisation

Fraud 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 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.

6.1 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.

"CVV2" means Card Verification Value and may be described as CVC, CVC2, CVV, CVV2 or CID, being the 3 or 4 digit number on a Nominated Card.

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.

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

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), Argentina, Spain as well as Indonesia.
- **Multiple card details**: When multiple card details (in particular international cards) are presented for a single transaction 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 section 4.5 "Refund" below 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.
- 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.

6.2 3D-SECURE – ONLINE AUTHENTICATION TOOL

'Visa Secure' and 'Mastercard Identity check' are collectively referred to as 3D-Secure. 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, a Visa Secure and, Mastercard Identity Check 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. Worldline Global Online Pay provides Merchants with 3D-Secure capability to enhance protection against online fraud. With this feature, customers making purchases through the Worldline Global Online Pay will have their transactions validated with the latest security standards, ensuring the safety of their personal and financial information. Please note that if transactions are forced through for processing without being authenticated by 3D-Secure , the Nominated Card Scheme may impose an additional charge that the merchant will be liable to pay.

Merchants utilising 3D-Secure are protected from receiving certain fraud-related Chargebacks. For example: where a cardholder disputes a transaction as unauthorised as they didn't initiate the transaction.

Please note that if Worldline Global Online Pay does not receive a response from the Nominated Card Scheme during an 3D-Secure transaction, Worldline Global Online Pay may still process the transaction.

Merchants should check with Visa Secure or MasterCard Identity Check for further information regarding whether fraud liability protection will still be available in these circumstances.

For further information about Visa Secure, and Mastercard Identity Check , please contact ANZ Worldline Payment Solutions on 1800 039 025.

6.3 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 and Mastercard rules and be open to possible fines
- unwillingly committing, and becoming involved in, fraud
- Your Merchant facility may be terminated.

6.4 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.

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 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.

7.1 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

7.2 VALIDATING PCI DSS COMPLIANCE

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

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

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.

7.3 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, for Visa and Mastercard 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.
- Once a transaction is processed, for multi-network debit obscure all digits except the first 6 and last 3 digits of the credit card Number (e.g. 1234 56XX XXXX 789) 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.
- 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.
- 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 Condition 38 'Information collection, storage and disclosure by the Merchant'.

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.

8. 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.

8.1 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. It is also recommended to display it on the website to assist with defending Chargebacks
- 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.

8.2 CARD ON FILE FOR RECURRRING AND INSTALLMENT TRANSACTIONS

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

When processing card on file recurring & installment transactions Merchants must:

Cleary disclose the basic terms of the subscription at the point of payment and capture the cardholder's affirmative acceptance of such terms.

The disclosure must include the price that will be billed and the frequency of the billing (for example, "You will be billed AUD $9.95 per month until you cancel the subscription.").

Merchants that utilise a negative option billing model must also disclose the terms of the trial, including any initial charges, the length of the trial period, and the price and frequency of the subsequent subscription (for example, "You will be billed AUD $2.99 today for a 30-day trial. Once the trial ends, you will be billed AUD $19.99 each month thereafter until you cancel.")

– For electronic commerce (e- commerce) Merchants, the point of payment includes the screen where cardholders enter their card credentials and any screens that show a summary of the order (such as a shopping cart) before it is submitted for authorisation by the cardholder.

Send a confirmation by email message or by any other electronic method at the time of enrollment in a subscription/recurring billing plan that provides the terms of the subscription, including the terms of a trial period when applicable, and clear instructions about how to cancel the subscription.

Merchants must send a receipt by email message or by any other electronic method after every billing that includes clear instructions for how to cancel the subscription. Cardholders may choose to opt-out of receiving these notices.

Note - Providing a link to another page that contains this information (such as a terms and conditions page), or otherwise requiring the cardholder to expand a message box or scroll down the page to see the terms, will not satisfy this requirement.

8.3 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.

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.

8.4 TOKENISATION – ONLINE SECURITY TOOL

(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.

If a cardholder selects 'remember my card details' the cardholder's card details will be tokenised and their details will be stored within our systems so that they do not need to re-enter their payment details upon the next checkout. The cardholder will need to notify the merchant if they no longer want to have their card details tokenised and stored in our systems. The action to delete the cardholders token will be managed by the merchant. The merchant will need to remove the cardholders token by following the instructions within the Delete Token API section which can be found within the Worldline Global Online Pay Support Site

ANZ WORLDLINE
Payment Solutions

anzworldline.com.au

200.0458.02_AUS_EN/11.2023 Item No. AW2591 11.2023 WZ137478