ANZ Merchant Business Solutions

Merchant Operating Guide

December 2025

Contents

Getting started 3

Welcome to ANZ 3

How to contact us 3

Your key responsibilities 3

Which Cards should you accept? 4

Security checks to Validate a Nominated Card 4

Card Present and Card Not Present Transactions 5

Authorisation 6

Settlement procedures 6

Monthly Merchant Statement 7

Merchant Facility Terminal Message Guide 8

Frequently Asked Questions 9

How to process Transactions 10

How to process Transactions using a Merchant Facility Terminal 10

How to process a Refund 11

How to process Transactions using an Online Payment Gateway 12

How to process a Refund 13

How to process Transactions using IVR Authorisation and Settlement Service 13

How to process a Refund 14

Merchant Facility Terminal not working 15

Fraud Protection and Chargebacks 17

Fraud Protection and Minimisation Tips 17

Protecting account and Transaction information 18

Securing your Merchant Facility Terminal 19

Recurring Transactions 19

Chargebacks 21

Getting started

Welcome to ANZ

Welcome and thank you for choosing ANZ for your Merchant Facilities.

This Merchant Operating Guide will help you understand the operation of your Merchant Facilities and the acceptance of Debit Cards and Visa, Mastercard and UnionPay Credit Cards. If you want to extend the range of cards accepted to include American Express, Diners Club or JCB, please contact these companies directly.

We recommend that you and your staff read this guide and keep it accessible for future reference.

The Merchant Operating Guide forms part of your Agreement with us for Merchant Facilities and may be varied or replaced by us from time to time. Terms defined in the Terms and Conditions have the same meaning when used in this Merchant Operating Guide.

How to contact us

For service, financial or general enquiries:

- Call ANZ Merchant Business Solutions on 0800 473 453, or email nzmerchantbusiness@anz.com. If you're calling from overseas, please dial 0064 4 802 2777.

For telephone authorisation and settling of Credit Cards:

- Call the Credit Card Authorisation Centre on 0800 741 100.

For problems with your Merchant Facility Terminal:

- Call your Merchant Facility Terminal supplier.

Postal address:

- ANZ Merchant Business Solutions
  PO Box 2211
  Wellington 6140

Your key responsibilities

The tasks and procedures detailed below and in this guide must be completed for you and your staff to fulfil your responsibilities as a Merchant. You must:

- Follow all the instructions in this Merchant Operating Guide.
- Only process Card Present Transactions unless we've agreed you can process Card Not Present Transactions or any other Transaction types as detailed in your Letter of Offer and Acceptance.
- Check your Merchant Service Fee on your monthly Merchant Statement regularly to ensure you're paying the correct rate.
- Accept and validate all Nominated Cards presented for payment – see page 4 for more detail.
- Follow the correct Authorisation procedures.
- Ensure the Cardholder authorises all Credit Card Transactions by using a Personal Identification Number (PIN) or signing the Transaction Receipt unless the Transaction is by mail, telephone or Internet order or is a Contactless Transaction.
- Always follow Merchant Facility Terminal prompts.
- Not split a single Transaction into two or more Transactions.
- Not give cash out with Credit Card Transactions (including Refunds).
- Not impose a minimum or maximum amount on Credit Card or Debit Transactions.
- Retain paper or electronic records of all Transactions for 18 months. These must be kept in a secure place and destroyed by shredding into small pieces after 18 months.
- Be alert to possible Credit Card fraud and report all instances – see page 17 for more detail.
- Ensure the logos of the cards you accept are clearly displayed at your point of sale.
- Protect account and Transaction information and your Merchant Facility Terminal by conforming to the requirements outlined on page 18.
- For Card Not Present Transactions, never store the CSC values (these are the three digit card security codes on the reverse of Visa, Mastercard and UnionPay Credit Cards) after a Transaction has been authorised.

- If a Debit Card or Credit Card is accidentally left behind in your premises, you must:
  - retain the card in a safe place for a period of two Business Days; and
  - hand the card to the claimant only after having established the claimant's identity by comparing signatures with another card in the claimant's possession; or
  - if not claimed within two Business Days, cut the card in half and send it to ANZ Merchant Business Solutions, PO Box 2211, Wellington 6140.

Which Cards should you accept?

We can provide you with the ability to accept all Visa, Mastercard and UnionPay Credit and Debit Cards, and New Zealand issued Debit Cards as payment for your goods and/or services.

If your Agreement with us for Merchant Facilities includes the acceptance of Visa, Mastercard and UnionPay Credit Cards, you must accept all valid Nominated Cards bearing any of these logos without restriction on the amount of the Transaction. If you're applying a Surcharge Fee to Visa, Mastercard or UnionPay Credit Card Transactions you must advise the Cardholder and give them a chance to opt-out before processing the Transaction. You must also follow the procedures set out in clause 18 of the Terms and Conditions.

Note: UnionPay Cards may be co-branded with another card scheme (e.g. Visa). Co-branded cards will be processed via the alternate scheme to UnionPay.

Security checks to Validate a Nominated Card

The following checks must be made to ensure a Nominated Card is valid and can be accepted for payment. Failure to recognise a fraudulent card could result in a Chargeback (disputed Transaction) and a loss to your business.

Checks for Credit and Debit Cards

Most Credit and Debit Cards have the card details embossed on them.

- Embossing should be even with all numbers the same size and shape (1)
- Check that the card expiry date is valid (UnionPay cards may not have an expiry date or display '00/00' – the Merchant Facility Terminal will check whether the card is valid) (2)
- Ensure the Cardholder name is present and does not look like it has been tampered with (3)
- Check that the name on the card matches other information provided.
- Check that the signature matches the one on the back of the card when the Merchant Facility Terminal prompts for a signature or when processing an Electronic Off-line Voucher (Electronic Off-line Vouchers do not apply to UnionPay).

Note: Visa and Mastercard cards without embossing usually have the words 'Electronic Use Only' printed on them and must only be processed as an Electronic Transaction using a Merchant Facility Terminal.

Card numbers

These start with a:

- '4' for Visa and have a total length of 16 digits
- '2' or '5' for Mastercard and have a total length of 16 digits
- '3', '4', '5', '6' or '9' for UnionPay and have a length between 13–19 digits.

Chip

Where an electronic microchip is embedded on the front of the Card, check there is no evidence of tampering (4).

Signature panel

- You'll also notice there are three additional numbers on the signature panel known as the Card Security Code. These numbers are needed for Mail, Telephone or Online Payment Gateway Transactions (5)
- Check that there is a signature and no evidence of tampering (6).

Magnetic stripe

Check the card has a magnetic stripe on the reverse (7).

Card Present and Card Not Present Transactions

Transactions can either be Card Present Transactions or Card Not Present Transactions.

Your Letter of Offer and Acceptance details which types of Transactions you can accept.

A Card Present Transaction is where the Cardholder and their Nominated Card are present during the Transaction at your Premises or place of business. These Transactions are typically processed electronically via a Merchant Facility Terminal.

A Card Not Present Transaction is where the Cardholder and their Nominated Card are not present during the Transaction. They are typically Transactions for sales via a website or a mail or telephone order. These Transactions can be processed via an Online Payment Gateway, by manually entering the Credit Card details into a Merchant Facility Terminal or by using the IVR Authorisation and Settlement Service.

Card Not Present Transactions carry a higher risk of fraud because the Transaction is not authorised by a PIN or signature. Therefore, it's more difficult to verify the Cardholder as the legitimate user of the card. Before you can accept Credit Card payments for Card Not Present Transactions, you must have approval from us for this facility.

If we've approved your business to accept Card Not Present Transactions they must be processed in strict accordance with the Terms and Conditions, this Merchant Operating Guide and all the requirements set out in the Mail, Telephone and Internet Order Transaction Schedule. Any Card Not Present Transactions processed by your business without our agreement, or that breach any aspect of this Agreement, may be charged back to you.

Authorisation

All card Transactions must be authorised. An authorisation is our confirmation that, at the time at which a Transaction is processed, the card has not been reported lost, stolen or blocked for use, and that there are sufficient funds available to cover the cost of the Transaction. An authorisation does not guarantee payment. If, at a later date, the Transaction is found to be an Invalid Transaction, it may be charged back to you. See page 21 for more information on Chargebacks.

Authorisation procedures vary depending on the type of Transaction.

Card Present Transactions (excluding Contactless Transactions) require the Cardholder to enter a Personal Identification Number (PIN) into a Merchant Facility Terminal. For Visa and Mastercard Credit Card Transactions, if you get an 'Accept with Signature' terminal message, the Cardholder can also authorise the Transaction by signing the Transaction Receipt. For UnionPay Transactions, a Merchant Facility Terminal will prompt a 'Signature Verified?' message and the Transaction will be authorised when the Merchant has confirmed verification by pressing 'Enter'. You must check the signature matches the one on the back of the card.

Card Not Present Transactions can be authorised electronically if they're manually entered into a Merchant Facility Terminal or processed via an Online Payment Gateway. If the Transactions are processed using the IVR Authorisation and Settlement Service, authorisation must be obtained by calling the Credit Card Authorisation Centre on 0800 741 100.

Note: 1. Card Not Present Transactions for UnionPay can only be processed through a Merchant Facility Terminal.

2. A Pre-authorisation Transaction for UnionPay must be completed within 30 days. After this period any Transaction will be declined by UnionPay.

Settlement procedures

Settlement is the term used to describe the transfer of funds into your Nominated Settlement Bank Account.

In most cases, you may set a time for settling your Merchant Facilities. The time period between 10.00pm and 11.00pm daily is not available as this is when we update your files to enable settlement of funds to your Nominated Settlement Bank Account. These accounts must be New Zealand-based transactional accounts, in New Zealand dollars.

We deposit the amount of your Transactions from Debit Cards and Visa, Mastercard and UnionPay Credit Cards into your Nominated Settlement Bank Account (see note below). The balances of Transactions from other cards, e.g. Amex/Diners, are deposited by the Card Issuer. The table below shows when you'll receive your settlement funds.

When your Merchant Facilities are settled	When funds are paid into your Nominated Settlement Bank Account
Before 10.00pm* daily	Funds processed overnight, available next morning
After 10.00pm* daily	Funds processed the following night, available the next morning

*8.00pm for ANZ eGate Transactions.

Note: UnionPay and Internet Transactions take an extra day to settle.

If you do not settle your Merchant Facilities within the time period chosen, we'll automatically settle it at the end of your Nominated Settlement period. However, a summary of Transactions will not be provided.

When you settle your Merchant Facility Terminal, always follow the steps detailed in your Terminal User Guide. The Terminal User Guide is provided by your terminal provider when they install your Merchant Facility Terminal.

If you need to know the value of Transactions completed through your Merchant Facility Terminal at a time other than at the end of your settlement period, you can request a Transaction Sub-totals Report. Instructions on how to request this are provided in your Terminal User Guide.

Monthly Merchant Statement

You'll be sent a Merchant Statement at the end of each month. The Merchant Statement details all Credit Card and Contactless Debit Card Transactions you've processed in the month. It also shows the Merchant Service Fee amount due. This is the fee we charge for processing your Credit Card and Contactless Debit Transactions. Your Merchant Service Fee is debited from your Nominated Charges Bank Account on the 12th of each month (or the following business day where the 12th is a weekend or public holiday) for the previous month's Transactions. You'll receive a Merchant Statement for each facility you have with us. For example, you would receive your Merchant Statement and be billed separately for a Card Present and Card Not Present facility.

Note: If you process UnionPay Online Payment Gateway Transactions, you'll receive a separate Merchant Statement for these Transactions. Transactions processed on the last business day of the month will appear on the following month's Statement. Refer to Settlement Procedures (page 6) for more information.

Merchant Facility Terminal message guide

When a Transaction is completed, a message will be displayed on the Merchant Facility Terminal. These messages tell you whether the Transaction has been accepted or declined and what action should be taken. Common messages are:

Terminal Message	Definition
Approved	The Transaction has been accepted
Invalid Account	The card is not loaded to access the account selected
Signature Required	A signature verification is required
Card Expired	The card's expiry date has been reached – don't pay out or release goods or services
Chip Declined	The Transaction wasn't approved – don't pay out or release goods or services
Declined – Contact Issuer	The Transaction wasn't approved – don't pay out or release goods or services. Ask the Cardholder to contact their Card Issuer
Do Not Honour	The Card Issuer will not allow the purchase. Tell the Cardholder that their Bank has not approved the Transaction – don't pay out or release goods or service
Incorrect PIN	The Cardholder has entered an incorrect PIN. Ask them to try again – don't pay out or release goods or services

Terminal Message	Definition
Invalid Amount	An incorrect 'cash-out' amount has been entered
Invalid Card	The card is not supported on the Switch – don't pay out or release goods or services
Invalid Transaction	The Transaction attempted is not supported on the card being used – don't pay out or release goods or services
Issuer Unavailable	The Switch can't contact the Card Issuer for an authorisation – do not pay out or release goods or services
Contact Issuer	The Transaction is not approved – don't pay out or release goods or services. Ask the Cardholder to contact their Card Issuer
PIN Tries Exceeded	The Cardholder has attempted the maximum number of PIN attempts. Seek another form of payment
Re-Try Transaction	Try the Transaction again – don't pay out or release goods or services

Frequently Asked Questions

What does the monthly Merchant Service Fee cover?

The Merchant Service Fee is paid to cover our costs for authorising and processing your Credit Card Transactions and crediting the funds to your Nominated Settlement Bank Account. The Merchant Service Fee also helps cover costs for our Merchant Business Solutions Helpdesk to answer any queries you may have.

How is the Merchant Service Fee calculated?

The Merchant Service Fee is often calculated as a percentage of the total dollar value of Credit Card Transactions processed for your business during the month and the average ticket size (sale). Fixed rates may be provided on request. Generally, a minimum monthly fee applies.

For Interchange Plus pricing, the Merchant Service Fee is calculated as the actual interchange fee plus a margin that includes the cost to process the Transaction. The cost includes scheme fees, network fees, float costs and an acquirer margin.

Are the funds credited to our account guaranteed?

If the Transaction has been properly authorised and the Transaction successfully completed, we'll credit cleared funds to your Nominated Settlement Bank Account. However, this payment may still be reversed later if a Chargeback event occurs, or the Transaction is later discovered to be an Invalid Transaction. For details, refer to the section on Chargebacks – see page 21.

How can I change merchant information?

If you need to change any of the information that you initially provided to us, call ANZ Merchant Business Solutions on 0800 473 453.

Who pays the cost if one of our employees uses a card fraudulently?

Your business may be financially responsible for any card fraud, whether carried out by an employee, a Cardholder or both in collusion. To reduce the risk, ensure the rules outlined in this guide are explained to staff, and follow the tips for detection in the section on fraud – see page 18.

Can I charge for processing?

You can apply a Surcharge Fee to some or all Visa, Mastercard and UnionPay Credit Card Transactions. If applying a Surcharge Fee, you must comply with the procedures set out in clause 18 of the Terms and Conditions.

Can I give cash out with a card Transaction?

Cash can only be provided to customers making Debit Transactions. You must not provide cash to a customer on a Credit Card Transaction under any circumstances. It is recommended that the customer be asked to sign the receipt as proof of receiving the cash.

Note: Cash-out is not available for UnionPay Transactions.

How to process Transactions

How to process Transactions using a Merchant Facility Terminal

Card Present Transactions

Once the Nominated Card has been validated for payment, enter the Transaction type and amount into the Merchant Facility Terminal and press enter. For more information about security checks and how to validate a Nominated Card for payment, please refer to page 4.

- If the presented card has a chip, process the Transaction by inserting the card into the Merchant Facility Terminal and remove only after the Merchant Facility Terminal says, 'remove card'.
- If the presented card doesn't have a chip, process the Transaction by swiping the card through the magnetic swipe reader on the Merchant Facility Terminal.

If the presented Card has a Visa PayWave, Mastercard Contactless or UnionPay QuickPass logo visible and your Merchant Facility Terminal supports Contactless Transactions, the Cardholder can process the Transaction by tapping their card on the Merchant Facility Terminal Contactless Reader. For more information about contactless payments please refer to the 'Contactless Transactions' section on this page.

Credit Card Transactions

- For all Credit Card Transactions which aren't contactless, the Cardholder can authorise the Transaction by either using a Personal Identification Number (PIN) or by signing the Transaction's receipt. Ensure that the signature on the back of the card matches the signature on the Transaction's receipt.

If a PIN is being used to authorise the Transaction and it's successful, an 'Accepted' message will appear on the Merchant Facility Terminal. If the Cardholder is signing for a Visa or Mastercard an 'Accepted with Signature' message will appear on the Merchant Facility Terminal. Check the signature and, if satisfied, complete the Transaction.

- For any Credit Card Transactions using a UnionPay card (except Transactions that are a Contactless Transaction of NZ$200 or less), the Cardholder must sign the Transaction's receipt. A 'Signature Verified?' message will appear on the Merchant Facility Terminal. Check the signature and, if satisfied, press 'Enter' to complete the Transaction.
- If a 'Declined' message appears on the Merchant Facility Terminal, the Merchant can ask the Cardholder for an alternative form of payment or retain the goods.

Debit Transactions

- All Debit Transactions (unless the Transaction is a contactless payment of NZ$200 or less) must be authorised by the Cardholder using a PIN.
- An 'Accepted' message will appear on the Merchant Facility Terminal if the Transaction is successfully authorised.
- If a 'Declined' message appears on the Merchant Facility Terminal, the Merchant can ask the Cardholder for an alternative form of payment or retain the goods.

Note: UnionPay Debit Cards may not have an expiry date or display '00/00'. Your Merchant Facility Terminal will determine the validity of the card.

Contactless Transactions

When your Merchant Facility Terminal is contactless enabled:

- If the value of the Transaction is NZ$200 or less, a PIN or signature is not required.
- An 'Accepted' message will appear on the Merchant Facility Terminal once the card or Mobile Wallet has been tapped on the card reader and the Transaction has been successful.
- If the value of the Transaction is over NZ$200, a PIN or signature is required to authorise the Transaction (unless the Transaction is a Mobile Wallet Transaction). If a PIN is used, an 'Accepted' message will appear on the Merchant Facility Terminal to confirm if the Transaction has been successful. If a signature is being used to authorise the Transaction, the Cardholder must sign the Transaction Receipt. An 'Accepted with Signature' message will appear on the Merchant Facility Terminal. Please check the signature and if satisfied, complete the Transaction.

- For any contactless Transactions over the value of NZ$200 using a UnionPay card, the Cardholder must sign the Transaction's receipt. A 'Signature Verified?' message will appear on the Merchant Facility Terminal. Please check the signature and if satisfied, press 'Enter' to process the Transaction.
- Mobile Wallet Transactions may require verification by the Cardholder using a Consumer Device Cardholder Verification Method (CDCVM) such as passcode, pattern or Biometric ID. In these cases, an 'Accepted' message will appear on the Merchant Facility Terminal if the Transaction is successfully authorised. If the value of the Mobile Wallet Transaction is for more than NZ$200, a PIN may also be required.
- If a 'Declined' message appears on the Merchant Facility Terminal, the Merchant can ask the Cardholder for an alternative form of payment or retain the goods.

Note: For all UnionPay Debit Cards issued outside New Zealand, the NZ$200 contactless limit does not apply. The Merchant Facility terminal being used to process the Transaction will advise the Merchant what authorisation is required. Please follow Merchant Facility Terminal prompts.

Transaction Receipt

For all Card Present Transactions, please ensure the Cardholder receives the 'Customer Copy' of the Transaction Receipt. The Merchant needs to retain the 'Merchant Copy' of all Transaction Receipts in a secure location for 18 months.

Card Not Present Transactions

If a Transaction is manually entered into a Merchant Facility Terminal, it is called a 'Card Not Present Transaction'. If you need to process a Card Not Present Transaction, you'll need to do the following:

1. Obtain the Credit Card number and expiry date from the Cardholder.
2. Follow the instructions on the Merchant Facility Terminal screen and manually enter the Credit Card details into the Merchant Facility Terminal.
3. The Merchant Facility Terminal will seek an automatic authorisation:
   - If the Transaction is successfully authorised, an 'Accepted' message will appear on the Merchant Facility Terminal.
   - If a 'Declined' message appears on the Merchant Facility Terminal, the Transaction was unable to be processed successfully. The Merchant can ask the Cardholder for an alternative form of payment or retain the goods. You must retain the 'Merchant Copy' of all Transaction Receipts in a secure location for 18 months.

How to process a Refund using a Merchant Facility Terminal

If a customer is returning goods which had been paid for using either a Visa, Mastercard or UnionPay Credit Card, don't give the customer a cash Refund. Process the Refund back to the same card that was used for the original purchase.

Accept the return of goods or the cancellation of services unless you've clearly disclosed to the Cardholder prior to the time of the Transaction that you do not accept returns or cancellations (where this is permitted by the law).

Upon the return of goods (in full or in part), the cancellation of services, or if you agree to a price adjustment on goods or services purchased with a Nominated Card, you must:

- make the Refund, or partial Refund by way of price adjustment, to the original Nominated Card that was used in the purchase Transaction or a card issued by the same issuer to the same Cardholder; or
- where you're unable to provide a Refund to the original Nominated Card used in the purchase Transaction (e.g. the original Nominated Card is not available or you attempted a Refund and the authorisation request was declined), the Refund is required by law, or you are an airline, make the Refund in accordance with your policy for providing adjustments and Refunds. This may include cash Refunds or a Refund to another Nominated Card.

When processing a Refund, also Refund any Surcharge Fee levied on the Cardholder under the original Transaction. For partial Refunds, the Surcharge Fee must be pro-rated.

Where possible you should ask the Cardholder for a receipt which identifies the Nominated Card by means of a truncated Primary Account Number (PAN). Note that where a device (like a smart watch or mobile phone) was used to facilitate payment, the original Nominated Card may not be identifiable.

Provide the Cardholder with a copy of the Refund Transaction Receipt stating:

- the date of the Refund
- a description of the returned goods, cancelled services, or price adjustment made
- the amount of the Refund.

You must not:

- accept payment from a Cardholder for the purpose of depositing funds to the Cardholder's account
- process a Refund other than for the purpose of crediting funds to a Cardholder for returned goods, cancelled services, or a price adjustment related to a prior purchase
- refund an amount which exceeds the authorised amount of the original purchase Transaction except as may occur as a result of currency value fluctuations or when you agree to credit return shipping costs.

If the Merchant Facility Terminal being used has an approved Refund facility, use the Merchant Facility Terminal to process the Refund back to the same card used for the original purchase. For more information on how to Refund Transactions through a Merchant Facility Terminal, please refer to your Terminal User Guide.

To find out how to get an approved Refund facility for your Merchant Facility Terminal, please contact our Merchant Business Solutions team on 0800 473 453.

How to process Transactions using an Online Payment Gateway

If you are specifically authorised by us in accordance with clause 3(ii) of the Merchant Facility Terms and Conditions to accept a Nominated Card as payment for goods or services ordered via the Internet:

- in addition to any information set out in this Merchant Business Solutions Merchant Operating Guide and the Mail, Telephone and Internet Order Transactions Additional Services Schedule or as otherwise notified by us from time to time, your website must contain all of the following information:
  - a complete description of the goods or services offered
  - a returned merchandise and Refund policy
  - a customer service contact, including electronic address and/or telephone number and the physical address of your Premises
  - any export or legal restrictions (if known)
  - a delivery policy (including the delivery cost, if any)
  - a privacy policy (including your policy on dealing with Cardholder information)
  - security capabilities and your policy for transmission of Cardholder's details
  - the "Visa" logo, in full colour, to indicate Visa card acceptance
  - the "Mastercard" logo, in full colour, to indicate Mastercard acceptance; and
  - the "UnionPay" logo, in full colour, to indicate UnionPay acceptance.
- except with our prior written consent, the Transaction currency on your website must be in New Zealand dollars only.
- your country of domicile must be New Zealand.
- you must complete a Secure Internet Site Declaration to our satisfaction.
- you must, at your cost, arrange for your website to be prepared and maintained in accordance with our reasonable requirements, including those requirements applicable to Internet security standards or as set out by a Nominated Card Scheme or otherwise notified by us in writing from time to time; and
- you must, at your cost, immediately rectify any security or processing faults or issues with your website as identified by either:
  - you; or
  - us and notified to you.

Some Transactions may occur without a physical card being present, these are known as 'Card Not Present Transactions.' These Transactions can be processed by either the Cardholder entering their card details into a secure payment page from a website at the time of purchase, or by the merchant manually entering the card details into a secure payment page.

The screen will indicate if the Transaction has been successful at which time, you must dispatch the goods or make the service ordered available to the customer.

If the authorisation is not successful, the Merchant may contact the customer to ask for another form of payment or retain the goods.

For more information about how to process a Transaction on your approved Online Payment Gateway, please refer to your Online Payment Gateway User Guide.

In certain circumstances Card Issuers may take further steps to identify and validate their Cardholders, often referred to as two-factor authentication. This is a matter between the Cardholder and the Card Issuer.

When processing Card Not Present Transactions via an Online Payment Gateway, your website must meet all the requirements set out in the Additional Services Schedule relating to Mail, Telephone and Internet Order Transactions which forms part of the Agreement. You must also comply with any requirements of the Nominated Card Schemes and the Payment Card Industry Data Security Standard as requested by us.

How to process a Refund using an Online Payment Gateway

If a customer is returning goods which have been purchased via an Online Payment Gateway with a Visa, Mastercard or UnionPay Credit Card, do not give the customer a cash Refund. Process the Refund back to the same card used for the original purchase.

If the Online Payment Gateway being used has an approved Refund facility, use the Online Payment Gateway to process the Refund back to the same card used for the original purchase. For more information about how to Refund Transactions through an Online Payment Gateway, please refer to your Online Payment Gateway User Guide.

To find out how to get an approved Refund facility for your Online Payment Gateway, please contact our Merchant Business Solutions team on 0800 473 453.

How to process Transactions using IVR Authorisation and Settlement Service

You may process a Card Present or a Card Not Present Visa or Mastercard Credit Card Transaction using the IVR Authorisation and Settlement Service if you don't operate electronic Merchant Facilities, and we have given you permission to process Transactions through the IVR Authorisation and Settlement Service.

To process a Transaction using the IVR Authorisation and Settlement Service follow the below steps:

1. Where the Cardholder is present, check their Nominated card can be accepted for payment. For more information about the security checks and how to validate a Nominated Card for payment, please refer to page 4.
2. Record your business details, the date, Cardholder name, card number, expiry date, Transaction amount, sales total and a brief description of the goods or services.

   Note: All Transactions must be in New Zealand dollars.
3. When the Cardholder is present, ensure the Cardholder signs the Sales Voucher and that you check the signature by comparing it against the signature on the Credit Card provided.
4. Authorise the Transaction by phoning the Credit Card Authorisation Centre on 0800 741 100 and have the following information available:

   - Your merchant number (9 or 11 digits) or PIN (last 5 digits of your merchant number)
   - Card number
   - Amount of the purchase
   - Card expiry date.

5. If the Transaction is successfully authorised; write the authorisation number you are given by the Authorisation Centre. Only once you've obtained authorisation should you provide the goods or services to the cardholder.

When using the IVR Authorisation and Settlement Service, your nominated Settlement Bank Account will be credited on the next business day.

- If the Transaction is declined or the card fails any validation checks, the Merchant can ask the Cardholder for an alternative form of payment or retain the goods.
- If the Authorisation Centre asks you to retain the card, please only do this if it can be done safely.

When processing a Card Not Present Transaction using the IVR Authorisation and Settlement Service, it's recommended that in addition to obtaining the card information required to complete the Transaction, that you also obtain the Cardholder's physical address, a contact telephone number, the name of the bank and the country the card was issued in.

We also recommend you ask for a written confirmation from the customer as a precaution against fraud. If you have a signed authority from the Cardholder to charge their Credit Card, we suggest you keep this on file for a minimum of 18 months in a secure location as it may be requested by us at any time to substantiate the Transaction.

Note: The IVR Authorisation and Settlement Service is not available for UnionPay Transactions.

How to process a Refund using IVR Authorisation and Settlement Service

If a customer is returning goods which had been paid for using either a Visa or Mastercard, do not give the customer a cash Refund. Please process the Refund back to the same card used for the original purchase.

If the original Transaction was made via the IVR Authorisation and Settlement Service, contact the Merchant Business Solutions team on 0800 473 453.

Additional Services

You may request a change in your Merchant Facilities at any time, including to add or remove any Additional Services. If we agree to change your Merchant Facilities, we'll issue an updated Letter of Offer and Acceptance confirming the Merchant Facilities to be provided and any associated fees or charges.

'Additional Services' means any of the following services or any new service offered by us under the Agreement:

(a) ANZ eGate

(b) Accommodation Transactions

(c) Car Rental Transactions

(d) Mail, Telephone or Internet Order Transactions

(e) Recurring Transactions

Merchant Facility Terminal not working

Your Merchant Facility Terminal may not work for a number of reasons, such as:

- a power outage
- technical failure with the hardware or software
- telecommunications failure
- a problem with the Switch.

A list of the most common reasons for your Merchant Facility Terminal not working, and the message it will display, are provided below.

Terminal Message	Definition
Comms Error	Telecommunications outage
Time Out	Communications or network fault
No Response from Host or Response Error	EFTPOS network outage
Unable to Process	Terminal hardware fault
Transmission Error	Phone line or other fault at site
System Fault	Host issuer's fault while authorising card
Power Failure	Power cut or failure

In the event the issue is a problem with the Switch or a telecommunications failure, Merchant Facility Terminals can perform Electronic Off-Line Transactions, also known as Electronic Off-Line Vouchers (EOV). When your Merchant Facility Terminal is in EOV mode the words 'EOV' or 'Offline' will be displayed on the terminal screen.

When processing Electronic Off-Line Transactions, the Merchant Facility Terminal will return an 'Accepted', Declined' or 'Signature Required' response. For those Transactions that require a signature, the Terminal will prompt you to confirm that you've verified the signature.

Select 'Yes' once the Cardholder has signed the 'Merchant Copy' of the Transaction Receipt, and you've verified the signature; the EOV Transaction will then be approved.

If you select 'No', the EOV Transaction will be declined and will print a Declined Transaction Receipt. You will not receive the funds from the Transaction.

Ensure you always retain the 'Merchant Copy' Transaction Receipt for your records and that it has been signed by the Cardholder when applicable.

You may process Electronic Off-Line Transactions when your Merchant Facility Terminal is not connected to the Switch due to a fault or connectivity issue. However, not all card types are supported in EOV mode including UnionPay cards.

When processing Electronic Off-Line Transactions, the Transaction is stored in the Merchant Facility Terminal's memory, which will later be processed when the connection to the Switch is restored. The Merchant Facility Terminal will attempt to connect to the Switch every 10 minutes.

Please note, you can only process Electronic Off-Line Transactions when:

- the Cardholder is present at the time of the Transaction
- the Transaction does not include any cash-out component
- the Transaction Receipt is signed by the Cardholder (when a signature has been requested), and the signature is comparable with the signature on the card, or if prompted the Cardholder enters their PIN
- the Transaction is not a Refund Transaction
- the Transaction is not greater than $300.

The Merchant copy of the Electronic Off-Line Transaction Receipt must be stored securely for 18 months as it may be requested by the cardholder's bank to verify the Transaction.

You should also be aware that:

The Card Issuer can apply an EOV Transaction limit to a chip card, and if this is less than the EOV limit set on the terminal, the Card Issuer's limit will prevail, and the card may decline in an EOV Transaction. The Card Issuer may also restrict whether the card can be used in an EOV Transaction.

Terminals connected to the Verifone network can process and store up to 200 Transactions a day up to a total maximum value of $5,000 for Credit and/or Debit Card Transactions. When this limit is reached, no further Transactions can be processed until the terminal is reconnected to the Verifone network, or the terminal limit is reset (the terminal limit resets each day at midnight).

Terminals connected to the Worldline network can process and store up to 99 Transactions in EOV mode at any one time. Should a terminal reconnect to the Worldline network and some or all of the Transactions are processed, and the terminal relapses into EOV mode, then additional Transactions (up to 99) can be processed and stored in the terminal.

If the terminal fails to upload stored Transactions when the connection is fixed, please contact the ANZ Merchant Business Solutions Helpdesk on 0800 473 453 for instructions on how you may be able to process the Merchant copy of the Transaction Receipts. Please note that if Transaction Receipts are not retained under these circumstances, you will be liable for any related losses.

Fraud Protection and Chargebacks

Fraud Protection and Minimisation Tips

Fraud can be committed by people using stolen Credit Card details, employees, or both acting in collusion, and can cause significant financial and reputational loss for your business. Your business is liable for all card fraud committed through your Merchant Facilities.

If a Credit Card Transaction turns out to be fraudulent, it may be charged back to you, and it could end up costing your business more than the original sale. High Chargeback levels can also attract penalties from the Nominated Card Schemes, including fines, and could result in the termination of your Merchant Facilities.

The more you know about the potential risks, the more you'll be able to protect your business against fraud and costly Chargebacks. Some Transactions carry a higher risk of fraud than others.

Higher-Risk Transactions

- Card Not Present Transactions – particularly from:
  - first-time customers
  - email orders
  - phone orders
  - mail orders
  - internet orders
- Manually entered Transactions – where the Credit Card number is manually entered into the terminal instead of swiping or inserting the card.
- Transactions where an authorisation has not been obtained.

Lower-Risk Transactions

- Card Present Transactions where the Transaction is completed through a Merchant Facility terminal.
- Internet Transactions authenticated via Verified by Visa or Mastercard SecureCode, or other forms of two-factor authentication (a security process where the Cardholder is required to provide further forms of Identification to the Card Issuer).

In providing you with suggestions on how to reduce the risk of fraudulent Transactions in your business, we make no representation as to the effectiveness of those suggestions or guarantee a reduction in or protection from fraudulent Transactions.

Card Not Present Transaction Fraud

If you've been approved by us to process Card Not Present Transactions, the recommended steps below can help you identify and reduce the risk of Card Not Present fraud in your business.

- In addition to obtaining the card information required to complete the Transaction, i.e. Credit Card number, expiry date and Cardholder name, also ask for the Cardholder's physical address, a contact telephone number, the name of the bank and the country the card was issued in.
- All Card Not Present Transactions, regardless of their value, must be authorised. Authorisation confirms that funds are available, and the Credit Card has not been reported lost or stolen. An authorisation does not guarantee payment or that the Cardholder is the legitimate user of the Credit Card. If a Transaction is later found to be fraudulent or disputed by the Cardholder, it may become subject to a Chargeback.
- Monitor your Transactions regularly – keep an eye out for any recurring or sequential data elements. Look for Transactions that might be 'testing' your system (e.g. many sales to the same address).
- Be wary of sending goods to overseas addresses.
- Be wary of orders originating from free email services, i.e. Yahoo, Hotmail, Gmail. They do not require a billing relationship or verification that a legitimate Cardholder opened the account.
- Be wary of urgent orders. Fraudsters will often want their illegally obtained items as soon as possible for quick resale.
- Be wary of orders shipped to a single address but made on multiple cards. Also check for multiple Transactions on one card or similar cards with a single billing address, but multiple shipping addresses.
- Don't send goods that are not part of your core business.
- Develop and maintain customer databases to track buying patterns and identify changes in buying behaviour.

- For telephone orders, wait a short period of time after the call is terminated, then call the given telephone number and ask for the caller. Confirm details of the order and record the date and time you spoke with the customer.
- If a courier delivers the goods, ensure the courier company returns the delivery acknowledgment so the signature of the recipient can be verified. Ensure goods are not left at vacant premises or left with a third party.
- If the Cardholder collects the goods, ensure the following:
  - The Credit Card is presented at the point of collection.
  - Check that the name on the Credit Card is the same.
  - The Credit Card security features are checked.
  - The Cardholder signs the delivery acknowledgment form.
  - The signature is the same as that on the back of the Credit Card.
  - Ask for suitable identification (photo ID preferable).
  - Be suspicious if someone collects goods on behalf of the Cardholder.

Card Present Transaction Fraud

Individuals using Credit Cards fraudulently in Card Present Transactions often behave unusually. While the following behaviours do not necessarily indicate criminal activity, be alert for customers who:

- make indiscriminate purchases without regard to size, colour or price
- are unnecessarily talkative or delay a selection repeatedly, until you're flustered
- hurry you at closing time
- purchase an extended warranty without hesitation even though it may be costly
- refuse clothing alterations even though they are included in the price of the garment
- make purchases, leave the store, and return a short while later to make additional purchases
- pull the Credit Card out of a pocket rather than a wallet.

Always use common sense as your guide - but if you're suspicious of a customer's card, please ask the customer to pay by other means, this could be by bank transfer, cash or another card.

You should never make any physical attempt to prevent a suspicious customer from leaving your Premises.

Employee Fraud

Be alert to changes in employee behaviour or sudden evidence of an increase in their wealth and take the following steps to reduce the risks of employee fraud in your business.

- Restrict access to your Refund and Card Not Present PINs and/or card details.
- Limit the number of employees with access to your merchant number.
- Always balance EFTPOS settlements and Refunds.
- Check your settlement amounts balance with the daily sales amounts (to check Refunds are not being inappropriately received).
- If your Agreement allows you to process manual 'key entered' Transactions into your Merchant Facility Terminal watch out for high volumes of these types of Transactions being processed through your terminal.
- Be wary of staff taking cash sales and balancing by processing fraudulent card Transactions.

Protecting account and Transaction information

If you accept Credit Card details from your customers or use a third-party service provider to do so (i.e. an Online Payment Gateway provider), you're responsible for ensuring that the customer's payment details are secure at all times.

The Payment Card Industry (PCI) Data Security Standard defines 12 industry best practices for handling and protecting Credit Card details. All businesses and third-party service providers that store, process or transmit Credit Card data must be compliant with the PCI standard. The PCI Standard details what needs to be protected and/or made secure and provides you with a framework of how to control the risks and keep Credit Card details that are in your possession safe and secure. The aim of the standard is to ensure a business, regardless of its size, follows good business practice for processing, storing and transmitting Credit Card details.

You must:

1. Install and maintain a firewall configuration to protect Cardholder data.
2. Not use vendor-supplied defaults for system passwords and other security parameters.
3. Ensure Credit Card information is never stored anywhere. Only retain the last four digits of the card number and ensure that the leading digits are not recorded.
4. Encrypt transmission of Cardholder data across open, public networks.
5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to Cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to Cardholder data.
10. Track and monitor all access to network resources and Cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for employees and contractors.

A full copy of the latest Payment Card Industry Data Security Standards is available online at: www.pcisecuritystandards.org

Further information is also available from the following websites:

- https://www.mastercard.co.nz/en-nz/business/merchants/safety-security.html
- https://www.visa.co.nz/pay-with-visa/security/fraud-prevention-tips-for-merchants.html

Recurring Transactions

You must obtain an authorisation for all Recurring Transactions and ensure you have the Cardholder's consent to process Recurring Transactions.

Where applicable, you must ensure the Nominated Card has a current validity date and that the CSC is provided when processing the first Recurring Transaction against that Nominated Card. After processing the initial Recurring Transaction, you must destroy the CSC in one of the manners set out in clause 8 of your Terms and Conditions.

If we and a Cardholder have authorised you to process Recurring Transactions, you must maintain appropriate business practices to ensure that the Cardholder's Nominated Card information remains current, accurate and complete (including the Nominated Card's expiry date where applicable). You must also comply with the terms and conditions for Recurring Transactions outlined in the Recurring Transactions schedule which forms part of the Additional Services Schedules.

For Recurring Transactions, you must provide Cardholders with a way to inform you of changes to their card account details and/or the Cardholder's wish to cancel payment arrangements. You're required to action any Cardholder request to change and/or cancel payment arrangements with five (5) Business Days of receipt of the Cardholder's request.

Recurring Transactions are invalid if the expiry date (where applicable) and CSC of the Nominated Card is not provided with the initial Recurring Transaction or if the Transaction is unauthorised and/or does not contain a Recurring Transaction flag.

Securing your Merchant Facility Terminal

All Merchant Facility Terminals are equipped with a number of in-built security features which are designed to help protect your customers' information. By implementing the recommendations below, you can help protect your business, your customers and your reputation from Credit Card and Debit Card fraud or misuse through your Merchant Facility Terminal.

Always ensure that your Merchant Facility Terminals are secure and under supervision during operating hours (including any spare or replacement Merchant Facility Terminals you have).

- Ensure that only authorised employees have access to your Merchant Facility Terminals, and they are fully trained on their use.
- When closing your store, always ensure that your Merchant Facility Terminals are securely locked and not exposed to unauthorised access.

- Never allow your Merchant Facility Terminal to be maintained, swapped or removed without advance notice from your terminal provider. Be aware of unannounced service visits and only allow authorised personnel to maintain, swap or remove your Merchant Facility Terminal, and always ensure that security identification is provided.
- Inspect your Merchant Facility Terminals on a regular basis – ensure that there are no additional cables running from your terminals and that the casing has not been tampered with.
- Check your Merchant Facility Terminal is located where it should be each time you open your store or premises and is printing the correct details on receipts.
- Record your Merchant Facility Terminal's serial number and store it in a secure location. Check the serial number matches this record each morning.
- Make sure that any closed circuit television (CCTV) or other security cameras located near your Merchant Facility Terminals cannot observe Cardholders entering details.

Contact ANZ Merchant Business Solutions on 0800 473 453 immediately if:

- your Merchant Facility Terminal is missing
- you or any member of your staff is approached to perform maintenance, swap or remove your Merchant Facility Terminal without prior notification from your terminal provider and/or security identification is not provided
- your Merchant Facility Terminal prints incorrect Receipts or has incorrect details
- your Merchant Facility Terminal is damaged or appears to have been tampered with.

Terminal Security

You must:

- only use a Merchant Facility Terminal of a type that has been approved by Payments NZ and the Switch the Merchant Facility Terminal is connecting to
- use the Merchant Facility Terminal for the purposes of the Agreement
- use the Merchant Facility Terminal in accordance with the Agreement and the supplier's agreement with you.

You must, at your cost, comply with all security requirements reasonably requested by us before, and as long as, the Merchant Facility Terminal is used for processing Transactions under the Agreement.

You must take proper care of and maintain regular servicing of the Merchant Facility Terminal.

Unless otherwise agreed you must arrange at your cost for an approved telecommunication supplier to install and maintain all necessary telecommunications infrastructure and associated services (including, for example, a telephone line or wireless communications device and any Internet services) to enable the use of the Merchant Facility Terminal. We are not responsible for maintaining any telecommunications requirements in connection with the Agreement.

You must arrange at your cost for the preparation of the location of the Merchant Facility Terminal in accordance with our requirements, including those requirements applicable to site security standards and suitable power supply.

The Merchant Facility Terminal site must enable the Cardholder to use the Merchant Facility Terminal keypad without the Cardholder's use of the keypad being observed by either security cameras, observation mirrors, reflective surfaces or by any other person, including by CCTV and internal monitoring devices.

You must use reasonable care and diligence to prevent and detect unauthorised use of any Merchant Facility Terminal.

You must take all steps that are, in the circumstances, reasonable to ensure that each Merchant Facility Terminal is protected against loss, theft, unauthorised access or use, modification or other misuse. You agree that such steps include ensuring that, at the start and at the close of business each day, each Merchant Facility Terminal is secure and has not been lost or stolen or tampered with in any way.

You must immediately notify us by telephone as soon as you become aware (or should reasonably have become aware) that a Merchant Facility Terminal has been stolen, lost or may otherwise have been altered, tampered with or compromised.

Any breach of this section by you may result in you being liable for any loss or costs suffered or incurred by us as a result of theft or loss of, or other breach of

security in connection with a Merchant Facility Terminal, including any loss arising from any unauthorised or fraudulent use of a Merchant Facility Terminal that occurs before you give notice to us in accordance with the clause.

If you:

- cease trading; or
- no longer require your Merchant Facility,

you must immediately terminate the Merchant Agreement by giving us 21 days' prior written notice in accordance with clause 25 of the Merchant Facility Terms and Conditions.

You must comply with all policies and procedures regarding Merchant Facility Terminal security as outlined in the Merchant Operating Guide.

Chargebacks

A Chargeback occurs when a Cardholder (or the Card Issuer) raises a dispute in connection with a Credit Card Transaction processed by you. You and your business are financially liable for all Chargebacks. If the dispute is resolved in favour of the Cardholder, the Transaction is charged back to you, and the value is debited from your Nominated Bank Account(s). As the Merchant, you could possibly lose the value of the sale as well as incurring a Chargeback Fee.

A Chargeback can occur up to 120 days (or 180 days for UnionPay) from the date a Transaction is processed, or from the date the goods or services were expected to be received by the Cardholder. We require you to store all Transaction Receipts for 18 months after the Transaction processing date. After 18 months, these should be destroyed by shredding them into small pieces.

If a Cardholder approaches you disputing a Transaction and you're unable to resolve the issue, you should refer the Cardholder to their Card Issuer.

If a Transaction is disputed, the Card Issuer that holds the account of the Cardholder in question will notify us and we'll notify you of the dispute. If our Transaction records cannot show sufficient proof of the Transaction, you'll be notified of the problem in writing and asked to respond in writing within seven (7) days with sufficient information to validate the Transaction.

If you do not lodge Transactions with us for settlement in accordance with clause 8 of the Terms and Conditions or if we reasonably determine that a Transaction involves one or more purchases made in the same Merchant establishment which have been split into two or more Transactions in an attempt to avoid the Authorised Floor Limit, or Electronic Off-line Payment Limit, the Transaction may be deemed invalid, and potentially subject to be charged back.

If you do not respond within seven (7) days, cannot provide sufficient proof of the Transaction, or we find proof that you've breached your Agreement, the Transaction may be charged back to you. If you're subject to an excessive number of Chargebacks, we reserve the right to charge for the processing of these disputes.

You can minimise the possibility of Chargebacks by following the procedures in this Merchant Operating Guide. For Card Not Present Transactions, protecting yourself can be challenging if a fraudster is intent on defrauding you. While we recommend you follow the procedures in this guide, the level of verification and fraud prevention measures you implement to reduce the chance of fraud is ultimately your decision. Usually, any fraud will manifest itself in the form of a Chargeback well after you have sent the goods.

The following list of Chargebacks includes, but is not limited to, the most common reasons why a Transaction may be disputed by a Cardholder, thus becoming the subject of a Chargeback:

- Processing errors
- Unauthorised use of card
- No signature on the Transaction Receipt or Sales Voucher
- Unauthorised Transaction
- Invalid card account number
- Incorrect Transaction amount
- Credit Card expired at time of sale
- Failing to respond to a retrieval request
- Goods not received by purchaser, wrong goods sent, or goods are defective.

There are additional reasons why a Transaction may become the subject of a Chargeback, and these are periodically determined by us and/or Visa, Mastercard and UnionPay.

Note: When prompted, a signature is mandatory on all UnionPay Credit Card Transaction Receipts.

anz.co.nz

ANZ Bank New Zealand Limited 12/25 250310_GMOG H261131