ANZ MERCHANT BUSINESS SOLUTIONS

MERCHANT OPERATING GUIDE
MARCH 2024

CONTENTS

Getting Started 2
- Welcome to ANZ 2
- How to Contact Us 2
- Your Key Responsibilities 3
- Which Cards Should You Accept? 4
- Security Checks to Validate a Nominated Card 5
- Card Present and Card Not Present Transactions 6
- Authorisation 7
- Settlement Procedures 8
- Monthly Merchant Statement 9
- EFTPOS Terminal Message Guide 10
- Frequently Asked Questions 11

How to Process Transactions 12
- How to process Transactions using an EFTPOS Terminal 12
  - How to process a Refund 14
- How to process Transactions using an Online Payment Gateway 15
  - How to process a Refund 15
- How to process Transactions using IVR Authorisation and Settlement Service 16
  - How to process a Refund 16

EFTPOS Terminal Not Working 18

Fraud Protection and Chargebacks 20
- Fraud Protection and Minimisation Tips 20
- Protecting Account and Transaction Information 23
- Securing your EFTPOS Terminal 24
- Chargebacks 25

GETTING STARTED

WELCOME TO ANZ

Welcome and congratulations on your decision to get your Merchant Facilities from us.

This Merchant Operating Guide is provided to help you become familiar with the operation of your Merchant Facilities and the acceptance of Debit Cards and Visa, Mastercard and UnionPay Credit Cards. If you wish 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 thoroughly 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 are 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 EFTPOS Terminal:

- Call your EFTPOS 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 Merchant Operating Guide must be completed for you and your staff to fulfil your responsibilities as a Merchant:

- Follow all the instructions in this Merchant Operating Guide.
- Only process Card Present Transactions unless we have 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 are 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 EFTPOS Terminal prompts.
- Do not split a single Transaction into two or more Transactions.
- Do not give cash out with Credit Card Transactions (including refunds).
- Do 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 21 for more detail.
- Ensure the logos of the cards you accept are clearly displayed at your point of sale.
- Complete all Transactions in New Zealand dollars unless we have given you permission to accept Transactions in another currency.
- Protect account and Transaction information and your EFTPOS Terminal by conforming to the requirements outlined on page 25.
- For Card Not Present Transactions, never store the CSC values (these are the three digit 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 are 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 21 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 card expiry date is valid (UnionPay cards may not have an expiry date or display '00/00' – the EFTPOS 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)
- Does the name on the card match any other information provided?
- Check the signature matches that on the back of the card when EFTPOS Terminal prompts for a signature or when processing an Electronic Off-line Voucher (Electronic Off-line Vouchers are not applicable 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 an EFTPOS 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).

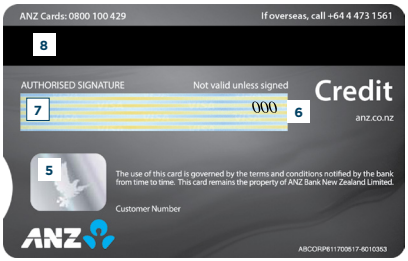
Note: UnionPay Cards may be co-branded with another card scheme (e.g. Visa).

Signature panel

- You will 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 (6)
- Check that there is a signature and no evidence of tampering (7).

Magnetic stripe

Check the card has a magnetic stripe on the reverse (8).



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 an EFTPOS 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 in to an EFTPOS 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 is 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 have 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 or 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 27 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 an EFTPOS 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, an EFTPOS 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 that on the back of the card.

Card Not Present Transactions can be authorised electronically if they are manually entered into an EFTPOS 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 an EFTPOS 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.

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 will 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: Customer Preferred Currency Transactions, UnionPay Internet Transactions and Multi-Currency Conversion Online Transactions take an extra day to settle.

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

When you settle your EFTPOS Terminal, always follow the steps detailed in your Terminal User Guide. This guide is provided by your terminal provider when they install your EFTPOS Terminal.

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

MONTHLY MERCHANT STATEMENT

You will be sent a Merchant Statement at the end of each month. The Merchant Statement details all Credit Card and Contactless Debit Card Transactions you have 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 will 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 Internet Transactions, Customer Preferred Currency Transactions or Multi-Currency Conversion Online Transactions, you will 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 for more information.

EFTPOS TERMINAL MESSAGE GUIDE

When a Transaction is completed, a message will be displayed on the EFTPOS Terminal. These messages advise you whether the Transaction has been accepted or declined and what action should be taken. Common messages are detailed in the following table:

Terminal Message	Definition
Approved	Transaction has been accepted
Invalid Account	Card is not loaded to access the account selected
Signature Required	Signature verification required
Card Expired	The card's expiry date has been reached – do not pay out or release goods or services
Chip Declined	The Transaction was not approved – do not pay out or release goods or services
Declined – Contact Issuer	The Transaction was not approved – do not pay out or release goods or services. Instruct the Cardholder to contact their Card Issuer
Do Not Honour	The Card Issuer will not allow the purchase. Inform the Cardholder that their Bank has not approved the Transaction - do not pay out or release goods or service
Incorrect PIN	The Cardholder has entered an incorrect PIN. Request them to try again – do not pay out or release goods or services
Invalid Amount	An incorrect 'cash-out' amount has been entered
Invalid Card	The card is not supported on the Switch – do not pay out or release goods or services
Invalid Transaction	The Transaction attempted is not supported on the card being used – do not pay out or release goods or services
Issuer Unavailable	The Switch cannot contact the Card Issuer for an authorisation – do not pay out or release goods or services
Contact Issuer	The Transaction is not approved – do not pay out or release goods or services. Instruct 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 – do not 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 covers 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. A minimum monthly fee will generally apply.

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 will 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 27.

How to 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 all 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 21.

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 21 of the Terms and Conditions.

Can I give cash out with a card Transaction?

You must not provide cash to a customer on a Credit Card Transaction under any circumstances. Cash can only be provided to customers making Debit Transactions. 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 AN EFTPOS TERMINAL

Card Present Transactions

Once the Nominated card has been validated for payment, enter the transaction type and amount into the EFTPOS terminal and press enter. For more information about the security checks and how to validate a Nominated Card for payment, please refer to page 5.

- If the presented card is a chip card, process the Transaction by inserting the card into the EFTPOS Terminal and remove only after the EFTPOS Terminal says 'remove card'.
- If the presented card does not have a chip, process the Transaction by swiping the card through the magnetic swipe reader on the EFTPOS Terminal.

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

Credit Card Transactions

- For all credit card transactions which are not 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 EFTPOS Terminal. If the Cardholder is signing for a Visa or Mastercard an 'Accepted with Signature' message will appear on the EFTPOS 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 EFTPOS terminal. Check the signature and if satisfied, press 'Enter' to complete the transaction.
- If a 'Declined' message appears on the EFTPOS 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 EFTPOS Terminal if the Transaction is successfully authorised.
- If a 'Declined' message appears on the EFTPOS 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 EFTPOS Terminal will determine the validity of the card.

Contactless Transactions

When your EFTPOS 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 EFTPOS 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 EFTPOS 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 EFTPOS 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 EFTPOS 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 EFTPOS 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 EFTPOS 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 EFTPOS terminal being used to process the transaction will advise the Merchant what authorisation is required. Please follow EFTPOS 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 an EFTPOS Terminal it is called a 'Card Not Present Transaction'. If you need to process a Card Not Present Transaction, you will need to do the following:

1. Obtain the Credit Card number and expiry date from the Cardholder:
2. Follow the instructions on the EFTPOS screen and manually enter the Credit Card details into the EFTPOS Terminal.
3. The EFTPOS Terminal will seek an automatic authorisation:
    - If the Transaction is successfully authorised, an 'Accepted' message will appear on the EFTPOS Terminal.

If a 'Declined' message appears on the EFTPOS 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 an EFTPOS Terminal

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

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

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

HOW TO PROCESS TRANSACTIONS USING AN ONLINE PAYMENT GATEWAY

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 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 had 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 5.
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 have 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 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 do this only if it can be done safely.

When processing a Card Not Present Transaction using the IVR Authorisation and

Settlement Service, it is 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.

EFTPOS TERMINAL NOT WORKING

Your EFTPOS Terminal may not work for a number of reasons:

- Power outage
- Technical failure with the hardware or software
- Telecommunications failure
- Problem with the Switch.

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

In the event the issue is a problem with the Switch or a telecommunications failure, EFTPOS Terminals can perform Electronic Off-Line Transactions, also known as Electronic Off-Line Vouchers (EOV). When your EFTPOS Terminal is in EOV mode the words 'EOV' or 'Offline' will be displayed on the terminal screen. When processing Electronic Off-Line Transactions, the EFTPOS Terminal will return an 'Accepted', Declined' or 'Signature Required' response. For those Transactions that require a signature, the Terminal will prompt you to confirm you have verified the signature.

Select 'Yes' once the Cardholder has signed the 'Merchant Copy' of the Transaction Receipt and you have 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 EFTPOS 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 EFTPOS Terminal's memory, which will later be processed when the connection to the Switch is restored. The EFTPOS 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.
- When a signature has been requested, the Transaction Receipt is signed by the Cardholder 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

Terminal Message	Description
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 PABX fault at site
System Fault	Host issuers fault while authorising card
Power Failure	Power cut or failure

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 every midnight).

Terminals connected to the Paymark network can process and store up to 99 transactions in EOV mode at any one time. Should a terminal reconnect to the Paymark 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 persons using stolen Credit Card details, employees or both 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.
- Transaction where an authorisation has not been obtained.

Lower-Risk Transactions

- Card Present Transactions where the Transaction is completed through an EFTPOS terminal.
- Internet Transaction 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 have 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 obtain 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, especially third-world countries.
- 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.
- Do not 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 are 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 PIN and/or card.
- 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 in to your

EFTPOS 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 Internet Payment Gateway provider), you are responsible for ensuring that the customer's payment details are secure at all times.

The Payment Card Industry 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 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. Do 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:

- www.mastercard.com/nz/merchant/en/security/what_can_do/SDP/merchant/index.html
- www.visa.co.nz/merchants/stayingsecuremerchants/accountsecurity.shtml

SECURING YOUR EFTPOS TERMINAL

All EFTPOS 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 EFTPOS Terminal.

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

- Ensure that only authorised employees have access to your EFTPOS Terminals and they are fully trained on their use.
- When closing your store, always ensure that your EFTPOS Terminals are securely locked and not exposed to unauthorised access.
- Never allow your EFTPOS 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 EFTPOS Terminal, and always ensure that security identification is provided.
- Inspect your EFTPOS 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 EFTPOS 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 EFTPOS Terminal's serial number and store it in a secure location. Check the serial number matches this record each morning.
- Make sure that any CCTV or other security cameras located near your EFTPOS Terminals cannot observe Cardholders entering details.

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

- Your EFTPOS Terminal is missing.

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

CHARGEBACKS

A Chargeback occurs when a Cardholder (or their bank) 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 in to small pieces.

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

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

If you fail to respond within seven days, cannot provide sufficient proof of the Transaction, or we find proof that you have breached your Agreement, the Transaction may be charged back to you. If you are 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, if a fraudster is intent on defrauding you, it is very difficult to protect yourself. While we recommend you follow the procedures in the guide, it is up to you to decide the level of checking and what processes you have in place to reduce the chance of fraud. 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 determined from time to time by us and/or Visa, Mastercard and UnionPay.

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

ANZ Bank New Zealand Limited 03/24 H24035

anz.co.nz