Merchant operating guide.

Merchant Business Solutions.

Card acceptance by business.

Contents.

1.0 About this booklet.

This is your Merchant Operating Guide for the acceptance of Mastercard, Visa credit and debit card transactions.

This booklet forms part of your Card Acceptance by Business Terms and Conditions and is designed to help you and your staff members become familiar with the use of your merchant facility.

You may also receive a Terminal User Guide and a Quick Reference Guide for transaction processing and other important information.

Why should I read this information?

It will help you use your terminal more efficiently, train your staff appropriately and help avoid costly errors.

1.1 Our contact details.

24/7 Helpdesk and Stationery Ordering.
1800 029 749

24/7 Authorisation Centre.
132 415

Note:

- Calls to 1800 numbers from a mobile phone will incur normal mobile phone charges.
- If you are using a terminal not supplied by us, please contact your terminal provider.

1.2 Merchant details: your handy reference.

Please complete the details below for your merchant facility.

Trading name:

Merchant number:

Floor limit:_____ For face to face transactions: $ _____

If your terminal is enabled for Electronic Fallback (EFB) transactions your floor limit is:

$_____for credit card transactions

$_____for debit card transactions

For mail/telephone order, instalment/recurring Transactions (for merchants where approved):

All Internet transactions: $0

The facility may not be taken outside of Australia at any time.

1.3 Honour cards with these symbols.

Your merchant facility enables you to accept any valid credit and debit cards showing the symbols below, whether the card is issued in Australia or overseas.

Credit/Debit card transactions:

Debit card transactions:

eftpos

The symbol may appear on the face or the reverse side of the presented cards. If you are in doubt please call our Helpdesk.

1.4 Look for the hologram.

Mastercard® hologram

Visa hologram

UnionPay hologram

Do not accept credit cards without holograms.

2.0 Understanding your EFTPOS terminals.

2.1 Terminal information.

Terminals that support debit card transactions incorporate a PINpad which allows cardholders to select their type of account (Cheque/Savings/Credit) and, where appropriate, input their personal identification number (PIN).

Locate the PINpad and terminal in a way that gives the customer privacy when inputting their PIN.

All EFTPOS terminals issued by us have a current Bank Certification and comply with all industry and regulatory requirements. EFTPOS terminals not issued by us must have a current Bank Certification and comply with all payment card industry and regulatory requirements.

You or your staff must never ask a cardholder to reveal their PIN.

2.2 Merchant Choice Routing.

When Merchant Choice Routing is enabled on an EFTPOS terminal, contactless Multi-Network Debit Cards are routed through the Australian eftpos network instead of the Visa or Mastercard networks. Transactions are therefore charged against the Debit Card Transaction Fee instead of the Credit Card Merchant Service Fee. A merchant may choose to send a contactless transaction via the debit network of their choice because that network may offer a lower cost for that transaction.

Note: Merchant Choice Routing can be enabled for certain EFTPOS terminals by contacting the Merchant Helpdesk or your Relationship Manager.

Recognising a Multi-Network Debit Card.

A debit card with a combination of either "Visa/eftpos" or "Mastercard/eftpos" logos.

Important information:

- Merchant Choice Routing is set at a Merchant Identification Number (MID) level and applies to all EFTPOS terminals connected to the MID.
- Enabling Merchant Choice Routing will result in changes to your fees and charges (cost savings are not guaranteed).
- For more information on Merchant Choice Routing, please refer to Clause 5.0 of 'Merchant Business Solution – Card Acceptance by Business Terms and Conditions' available on westpac.com.au/merchant-terms

What does Merchant Choice Routing mean?

It's an option that offers merchants more choice for accepting contactless debit card payments – with the ability to process the transaction via a debit scheme network that suits them.

2.3 Processing transactions guide.

Quick Reference Guides and/or Terminal User Guides are provided separately with your terminal. Please keep them where it is easily accessible. If you have not received your Quick Reference Guide (QRG), please telephone our Helpdesk for your copy. If you have not received your Terminal User Guide, please visit westpac.com.au or telephone our Helpdesk for your copy.

Important do's and don'ts:

- You or your staff must never ask a cardholder to reveal their PIN.
- You or your staff should not allow a cardholder to enter their PIN, until the transaction amount is displayed on the screen and is prompted to enter their PIN.
- For credit cards, compare the embossed card number on the face of the card with the number printed on the signature panel. Note that the number on the signature panel may be abbreviated to show only the last four digits of the card number, plus the CCV number. If these numbers do not match, retain the card and telephone the Authorisation Centre.
- Never request to retain the cardholder's card and/or PIN number. Retain the card only if advised by the Authorisation Centre operator.
- When our operator asks you to retain a card, ensure your personal safety. Disregard the request if it places you or anyone else at risk.

2.4 Refund password.

Enter your password prior to each refund transaction. You are responsible for protecting this password against unauthorised use.

Ensure that your password is changed regularly to prevent unauthorised use. To change your refund password, please contact the Helpdesk.

2.5 Security of your terminal.

Terminal copies of printed receipts must be handled by you and your authorised staff only. Keep your terminal where you can supervise its use at all times.

With the exception of Genie, E355, EFTPOS 1 and Presto Smart terminals, they must not be relocated without prior Authorisation from Westpac.

2.6 Terminal faults and problems.

If there is a systems fault or terminal problem, please refer to your Quick Reference Guide. Where your terminal displays a response code not listed on your guide, and you use an electronic terminal supplied by us, contact our Helpdesk.

If your terminal is enabled for Electronic Fallback (EFB), you can process:

- **Credit card transactions** which do not exceed your credit card floor limit.
- **Debit card transactions** which do not exceed your debit card floor limit.

Transactions exceeding this amount need a different payment method.

A floor limit is the amount of money above which credit card transactions must be authorised. The limit can vary from store to store.

What does EFB mean?

Electronic Fallback is the ability to continue performing transactions on the terminal, when online communication is down.

3.0 General merchant information.

3.1 Merchant statements.

Westpac will issue you a monthly merchant statement. UnionPay transactions will be provided on a separate statement. If you would like a single statement for all outlets, you can request a chain and headquarter statement by contacting the Helpdesk.

Dynamic Currency Conversion (DCC) is an option for your international customers to pay in their home currency. If you have received approval to process DCC transactions, you may receive a separate statement for these transactions.

Merchants must not offer DCC as the default payment option.

What are Chain and Headquarter statements?

Where more than one outlet is owned by one business, a separate statement outlining the month's trading for all outlets is available on request.

3.2 Merchant copies of all vouchers.

All physical and/or electronic copies of vouchers ('Merchant Copy') are for your records. You must retain copies for at least 18 months; however, government legislation may require you to keep them for longer periods (please check with the relevant authorities).

Failure to meet this requirement may result in 'chargebacks'. A chargeback is like a cardholder refund. It occurs when a cardholder disputes a transaction on their credit or debit card and asks for the charge to be reversed. The merchant provides a refund to the customer after the customer successfully challenges that charge.

You may have to refund a cardholder when you are unable to confirm details of a transaction.

3.3 Refunds, returned goods and exchanges.

Refunds may only be processed where there was an initial valid transaction on the same card. Merchants using EFTPOS terminals should refer to the Quick Reference Guide or User Guide for instructions on how to process a refund or exchange for their specific product type.

With credit/debit card transactions, remember never to refund cash in any instance.

3.4 Authorisation and Pre-Authorisation.

3.4.1 Authorisation.

An Authorisation only confirms the cardholder has funds available to cover the purchase, and the card has not been reported lost or stolen.

If you have an EFTPOS terminal, you can obtain an Authorisation using your terminal.

If you are an Internet merchant, an Authorisation request can be made via your Payment Gateway Service Provider.

When to obtain phone Authorisation.

You can also call the Authorisation Centre if:

- your terminal is processing a card transaction in electronic fallback mode and the amount exceeds your approved floor limit or your terminal otherwise prompts you to obtain an Authorisation;

- embossed card number on the face of the card does not match the number printed on the signature panel on the back of the card (note that the number on the signature panel may be abbreviated to show only the last four digits of the card number, plus the CCV number); or
- signatures do not match.

How to obtain phone Authorisation.

- Once your customer has handed over his/her card, remember to retain the card while you seek Authorisation. Please make sure the cardholder can see their card while it is in your or your employees' care. If you are asked to retain a card for any reason, carry out the instructions given by the operator. Remember that you should always ensure your personal safety and not place yourself or anyone else at risk.
- Phone the Authorisation Centre on 132 415 and provide the details requested.
- If approval is granted, the operator will give you an Authorisation number which you must enter in to the terminal.
- If declined, inform the cardholder to contact his/her financial institution for further clarification.
- Return the card to the cardholder unless our operator asks you to retain it.

Cancelling or changing amounts already Authorised.

Occasionally a customer may not proceed with a purchase after you have obtained Authorisation or you may have to amend the sale amount already authorised.

In both instances it is important that you telephone the Authorisation Centre to cancel the Authorisation(s) and to obtain a new Authorisation for any amended amount(s).

Note: If an amount is altered without the cardholder's signed authority the Authorisation will be invalid, and the transaction may result in a chargeback.

Hours of Authorisation.

The Authorisation Centre is available 24 hours a day, seven days a week.

3.4.2 Pre-Authorisation.

A Pre-Authorisation is an initial Authorisation for an estimated amount reserved on a credit card where the final billable amount is unknown at the initial point of sale. Instead of debiting funds from the cardholder you put the amount on a temporary "hold", locking those funds until the final billable transaction is processed. From this initial authorisation, subsequent Authorisation may be made, thereby reflecting the final amount agreed and acknowledged by the cardholder.

You must obtain additional Authorisation if the final amount exceeds the total authorised amount. You must also cancel any Authorisation(s) previously obtained that are no longer required.

A Pre-Authorisation does not protect you from the possibility of chargebacks. All other checks are your responsibility (please refer to Section 4.2 and 4.3 for mail/telephone.

Although we allow Pre-Authorisations to be made to attempt to ensure customers have funds to cover all expected expenses, you must obtain prior approval from your customer before any Pre-Authorisation is made. You must also advise the customer of the Pre-Authorisation amount.

Validity Periods.

Pre-Authorisations that hold funds on customers' cards even when the Pre-Authorisation should have been completed or cancelled are frequently the cause of cardholder complaints and disputes.

Mastercard Pre-Authorisations are held on the customer's account for 30 days. Once approved, the Pre-Authorisation can also be topped-up for additional amount or extended by 30 days if required.

For **Visa** transactions, the validity period of a Pre-Authorisation is determined by the type of business you have and how your Pre-Authorisation is processed. Refer to the table below for the validity period that applies to you.

How your Pre-Authorisation is processed?	Validity Period
Rental businesses performing Pre-Authorisation, e.g. boat rental, trailer park, bike rental; Transportation, Passenger railways and bus lines.	7 days
Hotels, Vehicle Rental, Cruise Lines performing Pre-Authorisation.	30 days
If you do not fall within either of the above industry types, your validity period will be based on one of the following scenarios:	
If the transaction is a recurring transaction, instalment transaction or prepayment.	1 day
If the transaction is not recurring or instalment or prepayment and you take a payment face-to-face.	1 day
If the transaction is not recurring or instalment or prepayment and you take a payment online, mail or over the phone.	7 days

You must process the final sale through as a 'checkout' transaction using the Authorisation(s) previously obtained. You must obtain additional Authorisation if the final amount exceeds the total authorised amount.

You must also cancel any Pre-Authorisation(s) previously obtained that are no longer required.

Please refer to westpac.com.au/preauthorisation and your Terminal User Guide for further information about any Pre-Authorisation requirements for your specific terminal.

3.4.2.1 Top up using a Visa card.

For hotels/motels, motor vehicle rental agencies, cruise lines, hospitality, rental businesses, transportation, passenger railways and bus lines, you may obtain top-up Pre-Authorisations for additional amounts above any amount already authorised after the check-in or rental pick-up date and prior to checkout or rental return date. You must obtain prior approval from your customers before any Authorisation is made.

An approved top-up Pre-Authorisation does not change the validity period of the original Pre-Authorisation nor the top-up.

For hotels/motels/cruise lines: the Pre-Authorisation amount can be based on the customer's intended length of stay at check-in time, and the room rate, including applicable tax(es).

For motor vehicle rental agencies: the Pre-Authorisation can be based on the cardholder's intended car rental period, the rental rate, distance rates and any applicable tax(es).

The estimated transaction amount should not include charges that cover potential vehicle damages or the insurance deductible amount.

Additional instructions for delayed or amended charges by car rental agencies.

You may process delayed or amended charges if the cardholder has agreed to cover these.

For any delayed or amended charges, you should process as a 'card not present' transaction and forward documentation to the cardholder.

Where a delayed or amended charge is disputed by the cardholder, you must provide us with all of the required supporting documentation within our required timeframe, as specified on the notice.

Traffic violation/parking charges: If the charge is for parking ticket or traffic violation, please process the transaction to the cardholder's account within 80 days of the violation or three business days after your payment of the penalty, whichever is the earlier. You need to hold a copy of the documentation issued by the relevant authority (e.g. police, council).

Rental vehicle damage charges: Process the transaction to the cardholder's account within 80 days of when the damage occurred, or three business days after your payment of repairs, whichever is the earlier. You need to hold all the relevant documents including:

- copy of the rental agreement;
- estimated cost of the damages from an authorised repair company. (The final amount of the transaction relating to the repairs may not exceed the Merchant's pre-authorised amount. If the actual cost of repairs is higher than the estimated amount, you must perform a top-up Pre-Authorisation amount);
- police accident report, where applicable;
- documentation showing the cardholder's consent to pay for damages with the card;
- copy of your insurance policy if you require the cardholder to pay an insurance deductible in case of damages.

Transactions may be successfully disputed if a receipt, specific to the damage, is not obtained.

3.5 Chargebacks.

A chargeback is like a refund. It occurs when a cardholder successfully disputes a transaction on their credit or debit card.

If the bank feels the cardholder's request is valid, the funds will be removed from the merchant's account and returned to the cardholder.

The most common reasons for chargebacks are:

Chargeback reason	Why this has happened
Unauthorised/Fraudulent Transaction	Cardholder did not authorise the transaction/s, transaction is fraudulent.
Cardholder does not recognise transaction	This can occur when a cardholder does not recognise your trading name on your credit card statement. Tip: You should always trade under the same name you have provided for your merchant facility and ensure it appears on your transaction receipts.
Authorisation for Transactions	Appropriate Authorisation was not obtained. This can occur when a transaction has been processed above the floor limit and Authorisation was not obtained. The chargeback may be raised under theses following conditions: • Account number not on file • Declined Authorisation • Expired card • No Authorisation • Cardholder/Issuer believe transaction has been processed incorrectly
Processing Error	Common scenarios under this chargeback reason: • Incorrect transaction amount/card number • Late presentment of the transaction • Transaction paid by other means. (i.e. cash or a different card)
Duplicate/Multiple processing	Cardholder claims transaction for same goods/services was processed more than once.
Non receipt of goods/ services	Cardholder claims goods/services for the transaction has not been received/rendered to the agreed-upon location or by the expected delivery date.

Invalid transactions will be charged back to your account. You will need to resolve the matter directly with your customer.

3.6 How to handle a chargeback or retrieval request.

If you receive notification of a chargeback or a retrieval request, you should reply promptly, within the timeframes we have specified in that request. A short letter or email providing details of the transaction should be sent, together with:

- the sales receipt (signed, where applicable);
- the order form or other sales record;
- the signed delivery receipt or other confirmation of delivery;
- any other supporting documentation.

Should you receive a chargeback or retrieval notification and you have already issued a credit for that transaction, you should email, fax or post copies of the credit refund documentation to us.

You must reply within the timeframes we have specified to a chargeback or retrieval notification to avoid being charged.

3.7 Cards left on premises.

If the card is not claimed within a reasonable period, cut it in half and dispose of it or hand it in at your nearest Westpac Branch.

If the card is claimed, verify the cardholder's identity before handing it over. If unsure, do not return it and dispose of it as suggested above.

3.8 Card faults.

If a faulty credit or debit card does not register through your terminal, advise the cardholder to contact their Issuer and seek an alternate means of payment or another card.

Manual keying in of credit card information is available for approved merchants; however, you could be liable for chargebacks.

3.9 Split ticketing.

If you 'split' a sale by completing two or more transactions to avoid having to obtain an Authorisation, it will result in the transactions being charged back to your Account.

For debit card transactions, using a terminal which is in EFB mode, you must not split a sale where the total amount of that sale is in excess of your debit card floor limit.

Under no circumstances should a sale be 'split' by completing two or more transactions, call the helpdesk for clarifications.

3.10 Stationery.

Re-order stationery at least one month prior to it being needed. Stationery will normally be delivered within 10 business days of us receiving your request. It is a good idea to carry six weeks requirements as a safety net. Call or order online from the dedicated Stationery system by visiting westpac.com.au/merchant-stationery

Store your thermal paper receipts away from heat and sunlight – it is the Merchant's responsibility to ensure that all transaction records are legible.

3.11 Ownership of stationery and terminals.

You will be charged for damaged, lost or stolen equipment. You must not sell any of these items, or give them to a third party, or allow access to a third party.

Unused promotional material remains the property of the Bank. Any unused promotional material must be returned to us immediately at the following address: **Merchant Business Solutions, GPO Box 18, Sydney NSW 2001.**

What happens when your merchant facility is cancelled?

We will collect your terminal from your premises.

4.0 Mail order and telephone order (MOTO) merchant.

4.1 First step: getting approval.

It is important that you gain prior approval from us **in writing** before you begin processing mail/telephone orders (MOTO transactions).

Mail order/telephone order transactions may only be processed for credit cards.

Points to remember when handling mail and telephone order.

1. **A sale must not be processed before the goods or services are provided.**
2. **Customer identification is your responsibility.** Illegal or dishonest (fraudulent) transactions will be charged back to your Account.

You will need to resolve the matter directly with the purchaser of the goods or services.

3. **Retain a signed copy of the cardholder's authority (mail order transactions)** for a minimum of 18 months, however, government legislation may require you to keep them for longer periods (please check with the relevant authorities).

It is your responsibility to establish a cardholder's identity, such as asking for valid photo identification. Authorisation will not guarantee payment or protect you from chargebacks.

4.2 Mail order advertisements and promotions: checklist.

You must include the following information on the customer order form (and authority):

Card details:

- cards accepted (Mastercard or Visa);
- card account number (16 digits);
- card valid from (where applicable) and expiry date.

Cardholder details:

- full name of cardholder, exactly as it appears on the card;
- cardholder's address and telephone number;
- signed statement from the cardholder, authorising the merchant to charge the purchase, or service, to the cardholder's Account.

Order details:

- details of goods/services ordered; cost of goods/services (including GST, if applicable).

Note: You must also include your business name and address.

Only approved Mastercard and Visa logos should be used in your advertisements. Call our Helpdesk for logo specification guides.

4.3 Telephone orders (for credit card payments) checklist.

Please keep a record of the following:

Card details:

- type of card (Mastercard or Visa);
- card account number (16 digits);
- card valid from (where applicable) and expiry date;
- for merchants transmitting CVV values, the CVV may be captured for transmission but **under no circumstances should the CVV be stored after transmission**.

Cardholder details:

- full name of cardholder, exactly as it appears on the card;
- cardholder's address and telephone number.

Order details:

- details of goods/services ordered;
- cost of goods/services (including GST, if applicable);
- the transaction date.

What is a 'card not present' transaction?

When the cardholder cannot physically present the card for inspection – such as online orders and mail orders.

4.4 Completing a sale where a card is not present (for mail/telephone orders).

Please complete the sale through your terminal and refer to your Quick Reference Guide and Terminal User Guide for further processing information.

5.0 Internet merchants.

5.1 Important things to remember.

To ensure customers to your site are provided with information they require to make transactions, your internet site must satisfy all of the following criteria:

- the trading name and the URL must not have any substantial differences in wording. This will maintain consistency and reduce any potential cardholder confusion;
- a clear and complete description of the goods and services offered for sale;
- contact information – trading name, Australian Business Number (where required), address, telephone number and fax number where available;
- a clear explanation of shipping practices (including overseas policy, if applicable) and delivery policy/timeframe;
- transaction currency: Westpac merchants can process and settle in AUD amounts only;
- total cost of the goods or services purchased, inclusive of all shipping charges plus GST where applicable;
- card scheme brand marks are displayed wherever payment options are presented;
- export restrictions (if any) – countries to which the merchant does not ship;
- a clear refund/return policy;
- consumer data privacy policy – advises what you plan to do with information collected from your customers;
- security capabilities and policy for transmission of payment card details;
- transmission policy;
- all transactions must be processed via secure PCI compliant encryption;
- each merchant domain name must utilise separate payment pages;
- all information must be accurate in all respects; and
- you must use digital certificates to establish a secure browser session between you and your customer;
- for transactions initiated via stored card information you must indicate that these are “Credential-on-file”.

Your website must not:

- contain anything that constitutes or encourages a violation of any applicable law or regulation, including but not limited to the sale of illegal goods or the violation of export controls, obscenity laws or gambling laws;
- contain any adult or pornographic content;
- offer for sale goods or services, or use to display materials, that may be considered by a reasonable person to be obscene, vulgar, offensive, dangerous, or are otherwise inappropriate;
- payment pages must be accredited by Westpac or an accredited service provider (of Westpac's choosing) and must follow our security requirements; and
- you should not change the types of goods or services sold through your merchant facility without first providing Westpac with a written notice, and then receiving written consent from Westpac confirming the change has been approved.

The internet poses specific risks to Merchants. Whilst the cardholder's details may be encrypted and online Authorisation received, the Authorisation does not ensure chargeback relief.

It is essential that you understand the term 'Authorisation' – what it means, and what it does not mean.

What Authorisation does mean:

- the account number is valid;
- the card has not been reported lost or stolen (although it may in fact be lost or stolen); and
- there are sufficient funds available to cover the transaction.

What Authorisation does not mean:

- an Authorisation does not confirm that the person providing the card number is the legitimate cardholder.

Although it is important to obtain an Authorisation for each transaction, it does not protect you from the risk of fraud or chargeback. Significant risk of fraud remains even though Authorisation has been obtained.

Online Authentication – 3D Secure.

Visa and Mastercard have jointly attempted to reduce this risk placed on internet merchants by developing an online cardholder authentication service known as 'Verified by Visa' and 'Mastercard® SecureCode™'. A term called '3D Secure' refers to the technology platform through which this service is offered.

Verified by Visa and Mastercard® SecureCode™ work as follows:

- a cardholder registers with their bank;
- the cardholder creates a password;
- cardholder browses merchant website and selects goods/services to purchase;
- when a cardholder attempts to make a purchase, a window pops up on screen requesting the cardholder to enter the password they previously created when registering with their bank. The 3D Secure software can detect if a card is enrolled or needs to be enrolled;
- for cards that are not able to support this service, the standard Authorisation process is followed;
- upon the cardholder entering the password, the information is routed to the cardholder's bank for verification. The result of the password verification check is then sent to the merchant, advising whether the purchaser entered the correct password. If the wrong password is entered, it is likely that the purchaser is not the rightful cardholder; hence, the merchant should not proceed with the transaction as liability then shifts back to the merchant.

The primary benefit to merchants of these verification processes is the chargeback liability shift that occurs. Subject to a few exceptions, if a merchant attempts to authenticate a purchaser using 3D Secure, both the cardholder and their bank may lose the right to make a chargeback claiming the cardholder did not authorise the transaction. This is irrespective of whether the cardholder or their bank subscribe to 3D Secure – all that matters is the merchant has implemented 3D Secure, and attempted to verify the cardholder's password.

If the password verification check fails (the purchaser entered the wrong password), you should not proceed with the transaction. If you proceed with the transaction after a cardholder has failed the verification check, you will incur the liability should a chargeback result.

While 3D Secure is available, there are still localised regions that do not support the liability shift. This allows global merchants to remain at some risk, as some transactions would not be covered by the use of this solution. Until such time as technology is widely available to certify use by the true owner, we strongly recommend that internet merchants make personal contact with the cardholder by telephone to confirm the transaction, especially for large sales.

5.2 Correct operation of an internet site.

Transactions conducted by cardholders via your internet site are processed automatically through connections between your site and us. We cannot guarantee that these services will be continuous, uninterrupted or without errors.

5.3 Internet gambling.

An online gambling merchant is a merchant that provides any form of gambling services over the internet or other networks. Gambling services include, but are not limited to:

- betting;
- lotteries;
- casino-style games;
- funding an account established by the merchant on behalf of the cardholder;
- purchase of value for proprietary payment mechanisms, such as electronic gaming chips.

If you are an online gambling merchant, your internet site must contain all of the following information:

- internet gambling may be illegal in the jurisdiction in which you are located; if so, customers are not authorised to use their payment card to complete this transaction;
- a statement of the cardholder's responsibility to know the laws concerning online gambling in the cardholder's country of domicile;
- a statement prohibiting the participation of minors;
- a statement promoting responsible gambling and awareness of gambling support associations (such as Gamblers Anonymous);
- a complete description of all of the following:
  - rules of play;
  - cancellation policies;
  - pay-out policies;
  - refund policies (even if your policy is not to refund, it must still be advised to your Cardholding customers);
- a statement recommending that a cardholder retain a copy of all transaction records and merchant policies and rules;
- you must not use the refund function to disburse winnings to cardholders.

6.0 Fighting fraud.

We have developed a separate brochure to assist you in fighting fraud. This brochure is entitled ‘Protecting business against credit card fraud’. If you do not have a copy, please telephone our Helpdesk.

Fraud prevention information is also available on the Westpac website at:

westpac.com.au/merchant-terms

This page has been left blank intentionally.

We're here to help.

24/7 Helpdesk and Stationery Ordering.
1800 029 749

24/7 Authorisation Centre.
132 415