Business Commercial Credit Cards

Account Access Conditions of Use

28 January 2020

bankwest

FOR BUSINESS

About These Conditions of Use

These Bankwest Commercial Cards Account Access Conditions of Use govern the use by Cardholders of their Bankwest Business Mastercard or Bankwest Corporate Mastercard and, where applicable, set out their rights and obligations regarding the use of their Card and PIN.

A Card allows the Cardholder to access the Card Account and any nominated Account through Bankwest Online Banking, Telephone Banking and Pay AnyBody.

You must read these Commercial Cards Account Access Conditions of Use together with the Letter of Offer incorporating the Financial Table and the Terms and Conditions specific to the Facility. All three documents, together with the application form, compromise your credit card contract with us. If there is an inconsistency between these Commercial Cards Account Access Conditions of Use, and the Terms and Conditions specific to the Facility, these Commercial Cards Account Access Conditions of Use shall prevail.

Mobile Wallets with which Cardholders can use a Card may be provided by technology companies and other third parties under their own service conditions. Bankwest does not impose any additional fees and charges for registering and using a Card with a Mobile Wallet provided by a third party. However, you will need to pay any third party fees and charges associated with downloading, registering and using the third party Mobile Wallet.

Bankwest is not liable for the use, functionality or availability of any third party Mobile Wallet or for any disruption to its availability whether through the failure of a telecommunications network or a contactless merchant terminal.

Usually, you will need to agree to the service conditions of the provider or a Mobile Wallet in order to register and use it with a Card.

Customer Enquiries

Please call 13 70 00 (24 hours, 7 days)

Where to Report Lost or Stolen Cards or Suspected Unauthorised Transactions (24 hours)

Within Australia

13 70 00 (cost of a local call)

Outside Australia

+61 8 9486 4130 (To use this reverse charges number please contact the international operator in the country you are in and request to be put through to +61 8 9486 4130. Please note: we have no control over any charges applied by the local or international telephone company for contacting the operator).

Contents

Part 1 - General

1.1 Definitions

In addition to the definitions in the Bankwest Corporate Mastercard and Bankwest Business Mastercard Terms and Conditions, the following definitions also apply to this document:

access method means a method the use of which we authorise and accept as providing authority to us to act on an instruction given through electronic equipment. A reference to an access method includes a reference to each of its individual components and includes, but is not limited to, a Card, Card details, a Security Token, a mobile device, a Mobile Wallet, a Biometric Identifier, a secret code or any combination of these. It does not include a method where a manual signature is the principal means of verifying the authority to give the instructions.

approved browser means a browser which can be used to access Bankwest Online Banking and Online Business Banking. A list of these browsers can be accessed at http://www.bankwest.com.au – enter 'browser' in the search box to find the list.

ATM means an automatic teller machine.

Biller means an organisation which tells you that you can make payments to it through the BPAY Scheme.

Biometric Identifier means a unique biometric trait, such as a fingerprint, which may be used to unlock a mobile device, change the setting on a mobile device or application for a Mobile Wallet, or initiate an EFT Transaction.

BPAY® scheme means a service which allows payment of BPAY payments electronically and receipt of or access to bills electronically via BPAY View. We have membership of the BPAY scheme. We will tell you if we cease to have membership of the BPAY scheme.

BPAY Pty Ltd means BPAY Pty Ltd ABN 69 079 137 518, GPO Box 3545 Rhodes NSW 2138. Tel: (02) 9646 9222.

BPAY View means an electronic service offered as part of the BPAY scheme which allows users to view bills from a nominated Biller electronically.

business day means a weekday including local public holidays but excluding holidays observed on a national basis.

Card means a Bankwest-branded credit card issued by us in accordance with the Business Mastercard or Corporate Mastercard Terms and Conditions.

Card Account means the account in the Accountholder's name which Bankwest sets up to record transactions made by users under the Facility.

Card details means the information printed on a Card and includes, but is not limited to, the Card number and expiry date.

Cardholder means each person to whom a Card has been issued at the request of the Accountholder to access the Card Account, and where the Accountholder is a natural person to whom a Card has been issued, includes the Accountholder.

Cardlink Services Ltd means Cardlink Services Ltd ABN 60 003 311 644, Level 4, 3 Rider Boulevard, Rhodes NSW 2138. Tel: (02) 8754 2800.

Credit Card scheme rules means the credit card scheme rules of Mastercard International Incorporated.

Customer Service Centre means a Bankwest-branded Customer Service Centre.

EFT system means a shared system under which EFT Transactions are processed.

EFT terminal means any terminal connected to the electronic banking system and authorised by us for use with an access method to conduct an EFT Transaction, including ATMs and EFTPOS terminals.

EFT Transaction means an electronic funds transfer from or to the Card Account initiated by a user through electronic equipment using an access method.

EFTPOS terminal means an electronic funds transfer point of sale terminal.

electronic equipment includes, but is not limited to, a computer, television, telephone, mobile phone, mobile device and an EFT terminal.

ePayments Code means the ePayments Code issued by ASIC.

Facility means the commercial card facility provided by Bankwest to the Accountholder and which is subject to these Commercial Cards Account Access Conditions of Use, the Letter of Offer incorporating the Financial Table, the terms and conditions specific to the facility and the application form.

merchant means a supplier of goods or services who accepts payment by Card.

mobile device means a mobile phone, tablet device or other small screen device which can be used to access the Internet.

Mobile Wallet means an application, loaded onto a mobile device, on which one or more Bankwest Cards may be registered to make transactions using near field communication or similar technology.

Nominated Account means a Bankwest-branded account with us, other than a credit card account, which you nominate and which we authorise users to operate by using their Card and PIN.

PAN means a personal access number of up to ten characters allocated to a user by us to identify the user for the purposes of accessing Telephone Banking and Bankwest Online Banking.

Password (also known as secure code) means the access method required by users, along with a PAN, to access Telephone Banking or Bankwest Online Banking. For Telephone Banking the password is a four-digit number. For Bankwest Online Banking the password is an alphanumeric code of 8-16 characters and in the form required by us as described in Bankwest Online Banking from time-to-time or, for those users with a Security Token, a 10-digit code which is a combination of the token PIN and token code.

PIN means the personal identification number we allocate a user for use with a Card, as changed by the user or us from time to time.

secret code means individually and collectively a user's

PIN, token code, password, token PIN, answers to your Secret Questions, SMS Code and code to unlock a mobile device, change settings or a mobile device or initiate an EFT Transaction on a mobile device.

Secret Questions means security questions pre-arranged with us that may be asked when you wish to perform certain transactions or use certain functions in Bankwest Online Banking. The correct answers must be provided before the transactions can be made or the functions used.

Secret Questions Security means the Security Setting where, when requested, you must correctly answer the Secret Questions, in addition to your existing password to authenticate you as a user;

Secured Online Shopping means the method by which purchases that are made on the Internet, using your Card with merchants that take part in the 'Mastercard SecureCode' or 'Verified by VISA' security system, are authenticated by requiring users to enter a SMS Code;

Security Setting means, your security setting for certain Secured Online Shopping transactions using your Card, SMS Code Security and for certain transactions in Bankwest Online Banking, SMS Code Security and/or Secret Questions Security, as applicable;

Security Token means, if we have provided one to a user, the physical device which generates a token code.

Services means Telephone Banking or Bankwest Online Banking, including the BPAY scheme or Pay AnyBody services.

SMS Code means a randomly generated six-digit code we send by short messaging service (SMS) to your mobile phone for conducting certain Secured Online Shopping transactions using your Card or to perform certain transactions or use certain functions in Bankwest Online Banking;

SMS Code Security means the Security Setting where, when requested, you must correctly enter your current SMS Code, in addition to any existing Password to authenticate you as a user;

Terms and Conditions means the specific Business Mastercard or Corporate Mastercard Terms and Conditions we provide to you together with these Account Access Conditions of Use and which we tell you

form part of the Card contract.

Token code means a random six-digit code generated by a Security Token. The security of a token code is breached if the Security Token is lost, stolen or allowed to be seen by any person other than the user.

token PIN means a four-digit code which is chosen by users who have been provided with a Security Token.

user means you and/or any Cardholder.

WST means Western Australian Standard Time.

we, us, the Bank or **Bankwest** means, Bankwest, a division of Commonwealth Bank of Australia ABN 48 123 123 124 AFSL/Australian credit licence 234945 and its successors and assigns. Any other grammatical form of the word 'we' has a corresponding meaning.

you means the Accountholder. Any other grammatical form of the word 'you' has a corresponding meaning. For the purposes of complying with the requirements for the SMS Code Security and the Secret Questions Security, where relevant, "you" also includes any user.

Unless otherwise required by the context, a singular word includes the plural and vice versa.

1.2 ePayments Code not applicable

The ePayments Code does not apply to EFT Transactions because the Card Account is an account maintained for business purposes.

1.3 Changes

We can change these Commercial Cards Account Access Conditions of Use at any time.

We will give you notice by writing to you at least 30 days (or such longer period required by law) before we:

(a) impose or increase charges relating solely to the use of an access method or the issue or use of any additional or replacement access method;

(b) increase your liability for losses relating to EFT Transactions;

(c) impose, remove or adjust a daily or other periodic transaction limit applying to use of an access method, the Card Account or electronic equipment; except where

an immediate change is necessary to restore or maintain the security of the EFT system or a Card Account.

Subject to any applicable legislation, we will notify you of other changes to these Conditions of Use no later than the day that the change takes effect by.

We may notify you of changes by:

(a) electronic communication to your nominated electronic address

(b) a SMS text message to a mobile number you have given us for contacting you;

(c) making the information available on our website after first notifying you by:

i. SMS message to a mobile phone number you have given us for contacting you;

ii. by electronic communication to any other electronic address you have given us for contacting you, or

iii. push notification from the Bankwest App

that the information is available for retrieval by you;

(d) a notice on or with your statement or account;

(e) publishing a press advertisement;

(f) notices on EFT terminals or in our Customer Service Centres or

(g) such other means as we agree with you.

Should we provide you with information by an electronic method, the information will be deemed to have been provided to you when the electronic communication enters the first information system outside Bankwest (e.g. your or your internet services provider's information system).

1.4 Cancellation of electronic access

If we believe it is reasonable to do so, we may suspend, limit or deny access to a user to the Services or the Card Account at any time without prior notice, for any reason, including (but not limited to):

- suspected fraudulent use;
- to comply with anti-money laundering and counter-terrorism financing laws;
- unsatisfactory account operation;

- non-compliance with these Account Access Conditions of Use;
- you have not complied with the requirements for your Security Setting; or
- if we consider a security issue has arisen which requires further investigation.

If in such circumstances we cancel a Card, you may request a replacement Card unless we decide not to provide you with further credit. In the event that electronic access to the Card Account is cancelled by you or us, you must, if relevant, stop the use of all Cards and any Security Tokens, returning the Security Tokens to us undamaged, together with the Cards which must be cut into several pieces.

You will remain liable for transactions made by a Cardholder prior to or after cancellation of their Card. In addition, a cancellation may not be effective until the Card has been returned to us.

1.5 Cardholders

You agree that you are responsible to ensure that Cardholders comply with these Commercial Cards Account Access Conditions of Use and to ensure that each Cardholder protects their access method in the same way as these Commercial Cards Account Access Conditions of Use require you to protect your access method.

1.6 Access to a nominated cheque or savings account

Access to a Nominated Account by a user is not governed by these Commercial Cards Account Access Conditions of Use but by the Bankwest 'Account Access Conditions of Use'. Users should refer to the Bankwest Account Access Conditions of Use for information about the use of the Card to access a Nominated Account.

You acknowledge that by linking a Nominated Account to a Card you increase the risk of loss for which you could be liable if the Card is used without a user's knowledge or consent. You agree that any user will have authority to operate a Nominated Account.

1.7 Privacy

(a) Each user acknowledges that we may collect personal information about them (including any mobile device of a User to which a Card has been loaded using a Mobile Wallet) for the purposes of providing our products and services and may use and disclose that information in accordance with the privacy consent they gave when they signed the application form for the Facility or a Card.

(b) Without limiting that consent, each user agrees that we may disclose personal and transactional information (including any mobile device of a User to which a Card has been loaded using a Mobile Wallet) to others in order to execute instructions given to us (including use of the BPAY scheme), including:

i. any party nominated to receive a payment;

ii. BPAY Pty Ltd and any agent appointed by it from time to time, including Cardlink Services Ltd who provides the electronic systems to implement the BPAY scheme;

iii. any party we may use in sending SMS Code to you; and

iv. agents and contractors we may use in providing any of our Services.

(c) Users may have access to the personal information we hold about them at any time by asking us.

(d) Users can request access to information held by BPAY Pty Ltd or its agent Cardlink Services Ltd using the contact details supplied in clause 1.1.

For more details of how we handle personal information, please refer to our Privacy Policy, available from our website **(bankwest. com.au)** or by telephoning us on **13 70 00**

1.8 Your Security Setting

Your Security Setting provides additional security where you engage in transactions that we consider can carry a higher risk. It assists in protecting your transactions in such circumstances.

Unless exempted by us in accordance with these Bankwest Commercial Cards Account Access Conditions of Use, all users must be registered for SMS Code Security when required by us. All users must notify us of

their current mobile phone number and inform us of any change in their mobile phone number by contacting us as follows:

Call the Business Customer Relationship Centre on **13 70 00.**

If you are registered for SMS Code Security, you need to ensure your mobile phone will be able to receive SMS Code.

Unless exempted by us in accordance with these Bankwest Commercial Cards Account Access Conditions of Use, all users of Bankwest Online Banking must be registered for SMS Code Security and Secret Questions Security when required by us.

We will notify you once you are registered with a Security Setting.

If you have difficulty receiving SMS Code from time to time (e.g. you are going overseas), contact us to apply for an exemption and we may change your Security Setting for an appropriate period approved by us. Any change we make to your SMS Code Security will apply to you conducting Secured Online Shopping transactions using your Card and also transactions in Bankwest Online Banking.

If you have an exemption from SMS Code Security for any period of time, your ability to make payments to third parties in Bankwest Online Banking may be limited.

We may suspend your SMS Code Security if we have reason to believe that your online security is at risk, e.g. you entered the wrong SMS Code more than once. If we do, your access to Bankwest Online Banking for any functions normally requiring a SMS Code to be entered including payments to third parties may be suspended or limited and will not apply until we reactivate it. For assistance, call the Business Customer Relationship Centre on 13 70 00.

Part 2 - Cards Conditions of Use

2.1 About this Part

This Part (together with Parts 1, 5, 6 and 7) applies to all transactions involving the use of a Card , Card details, or a Mobile Wallet to access the Card Account.

2.1.1 Use of the Card

(a) The Cards must be used solely for business purposes and not for private, household, domestic or residential investment purposes.

(b) A user must not use their Card for any unlawful purpose, including the purchase of goods and services prohibited by the laws of Australia and /or the laws of the location where the Card is used.

2.1.2 Selection/Issue of PIN

In Australia, Cardholders will usually need to enter a PIN to use their Card to access a Nominated Account.

A Cardholder may be required to select a PIN upon collection of the Card or we will allocate a PIN to the Cardholder when the Card is first issued.

A Cardholder may change their PIN at any time.

If a PIN is lost or stolen, the relevant Cardholder may select a new PIN or we may issue them with a new Card and PIN.

2.1.3 Card validity and expiry

(a) A Card is valid only if it is signed by the Cardholder and is used during the validity period shown on the face of the Card.

(b) The Cardholder must destroy any Card that is no longer valid, by immediately cutting it in several pieces and disposing of them securely.

2.1.4 Card re-issue

We may issue a new Card to a Cardholder at any time. All such Cards are subject to these Commercial Cards Account Access Conditions of Use. We reserve the right not to reissue a Card.

2.1.5 All Cards remain our property

Each Cardholder agrees that the Card issued to them remains the property of the Bank and agrees to return the Card to us on:

- Our request;
- Cancellation of the Card;
- Closure or termination of the Facility; or
- Termination of their authority to use the Card.

2.2 Access to the Card Account

(a) Over the counter (including EFTPOS terminals), mail order, telephone and online users can use their Mastercard in Australia and overseas over the counter at financial institutions and merchants displaying the Mastercard symbol. In Australia, Cardholders will usually need to enter a PIN.

If a merchant accepts payment with a Card by mail order, telephone or online, the Cardholder may authorise payment in the manner required by the merchant by providing the Card details to the merchant.

Where you are registered with SMS Code Security, you must enter your current SMS Code when requested for conducting certain Secured Online Shopping transactions using your Card.

(b) ATMs
Users may use their Mastercard and PIN to obtain cash advances in Australia and overseas at ATMs displaying the Mastercard symbol.

2.3 How much cash can a user get?

The minimum amount a user can obtain each day from Bankwest-branded ATMs is $20 or $50 (depending on the ATM), otherwise it will be determined by the institution from which the cash advance is obtained.

A maximum daily ATM transaction limit also applies. Users will be advised of this limit when their Card is issued. Other financial institutions, non-Bankwest-branded outlets and our agents may have additional limits.

Cash advances may not be obtained using EFTPOS terminals but are available at our Customer Service

Centres up to the amount of available credit.

Banks overseas displaying the appropriate Card symbol may arrange a cash advance in local currency from the Card Account. This is subject to their own cash advance transaction limit, their own country's exchange control requirements, any fees they may charge and your available credit limit.

A maximum monthly cash advance limit may apply. The amount of the limit will be at our discretion, may vary monthly and will be determined according to our credit risk assessment of you, the period for which the Facility has operated and your payment history.

2.4 Paying bills using a Card

Users can pay utility accounts such as water, gas and power from the Card Account by mail or telephone (if applicable) quoting their Card details. The transaction will be treated as a purchase by us.

If a user pays such accounts over the counter using their Card at a bank nominated by the utility, the amount will be debited to the Card Account as a cash advance (not a purchase) and will immediately be subject to interest charges. (Utility accounts can also be paid by way of BPAY payment – see clause 3.14).

2.5 Deposits

You can deposit funds to a Card Account with some of our agents and at any Bankwest-branded ATM with deposit capability. There are limits on the amount of cash you can deposit at our agents. If a cheque is deposited the proceeds of the cheque will not be available until the cheque is cleared.

Any cheques drawn on or deposited to your account, or bank cheque or other document deposited to your account or delivered to us in connection with a transaction on your account, becomes our property when we present the cheque or other document for payment (even if it is dishonoured) or when the transaction is otherwise complete but you retain all rights against the drawer and any endorser of any dishonoured cheque.

We will be responsible for the security of all deposits made at Bankwest-branded ATMs. The amount deposited is

checked by us and our count of funds deposited is regarded as conclusive evidence of the amount deposited. If the amount appearing on the transaction record differs from the amount actually received by us, we will credit the Card Account with the amount actually received and notify you as soon as possible. You must not include coins in payment envelopes at Bankwest-branded ATMs.

Cash deposited will not be available for withdrawal until after we have posted the cash amount to the Account.

2.6 Transactions at EFT terminals

When a user makes an EFT Transaction at an EFT terminal you authorise us to act on the instructions given by the user. Users should ensure that the correct transaction details are entered into the terminal before authorising a transaction and also that the completed transaction is in accordance with those instructions. All vouchers and transaction records should be kept to help check statements.

EFT Transactions may not be processed to the Card Account on the day they are made. Processing may take a number of days.

Users should observe the guidelines set out in clause 5.2 to ensure the security of access methods when transacting at an EFT terminal.

2.7 Do transactions have to be authorised by us?

Transactions on a Card Account may need to be authorised by us. We may in our discretion decline a transaction (or any category of transaction) for any reason, including but not limit to, security reasons, perceived risk of the transaction or if you have not complied with any SMS Code Security requirements, or if you are in default, your Facility or card spending limit would be exceeded, the transaction is not within the restrictions (if any), placed on the Card or we are unable to authorise the transaction because the system to do so is inoperative and the amount of the transaction exceeds limits we set in the circumstances.

Once an authorisation is obtained, it will reduce the amount of available funds for the Facility. If a user, or the merchant, does not proceed with a transaction after it has been authorised by us your available credit limit may be reduced for at least seven business days.

2.8 Use of Card at merchants, financial institutions or our agents

If a user provides a merchant with their Card details:

(a) to enable the merchant to complete a transaction in the future (e.g. authorises a car hire company to recover the cost of any damage to the hire car, excess mileage or fines, or authorises a hotel for room service or use of the mini-bar); or

(b) to pay for goods and services in advance even if the user later decides not to take the goods or use the services, the user authorises the merchant to complete the transaction and when the merchant completes the transaction the available credit limit will be reduced.

To the extent permitted by law, we do not accept responsibility for the actions of financial institutions, merchants or our agents:

(a) in refusing to accept or honour a Card; or

(b) in imposing limits or conditions on use of a Card.

The user must resolve such issues directly with the financial institution, merchant or agent. Card promotional material displayed on any premises is not a warranty by us, by any other financial institution or by merchants carrying on business there, that the goods and services on those premises may be purchased using a Card.

Unless required by law we are not responsible for goods or services supplied to a user or for any refund. The user must take up any complaints or concerns directly with the merchant and any refund is a matter between the user and the merchant.

If a merchant gives the user a refund we can only credit the Card Account when we receive correctly completed refund instructions from the merchant. Refunds credited to the account will not be treated as monthly payments to the account but will reduce the amount of the most recent outstanding purchases appearing on the next statement following the refund.

Care! If a refund is obtained from an overseas merchant, there may be a difference in the Australian dollar values due to movements in the foreign exchange rates. You take the risk of currency fluctuations between the date of purchase and the date of refund.

Care! You should obtain proof of refund and should check that the refund appears on the Card Account statement. The hours that a merchant, financial institution or our agents may be open for business will determine when a terminal at their premises will be available.

2.9 Use of Card with a Mobile Wallet

A Card may be used with a Mobile Wallet we approve for use form time to time to make contactless payments to Merchants and payments within Mobile Wallet applications.

If the dollar value of an EFT Transaction initiated using a Mobile Wallet exceeds the contactless payment threshold we set from time to time, a User may need to enter the PIN associated with the Card, to initiate the EFT Transaction. For some mobile devices, carrier-specific software settings may override Mobile Wallet settings so that the User may need to unlock the mobile device before the contactless terminal will allow the User to initiate an EFT Transaction.

Usually, a User must have selected the relevant Mobile Wallet as the default 'tap and pay' application on a mobile device's settings to transact using the Mobile Wallet and a User must have the Card selected as the default card within the Mobile Wallet in order to use the Card when making an EFT Transaction. If a Mobile Wallet is the default 'tap and pay' application on the User's mobile device settings, the User may only be able to pay using that Mobile Wallet application despite another 'tap and pay' application being open at the time the User taps the User's mobile device at the contactless terminal.

A Mobile Wallet may not work when a mobile device is not within range of a cellular or wireless internet connection and if the mobile device has not been connected to cellular or wireless internet for an extended period of time, there may be a delay before mobile device is reconnected.

How to add or remove a Card loaded to a Mobile Wallet:

Before we can allow a Card to be added to a Mobile Wallet:

- we must verify the User's identity; and
- the Card must not be closed or reported lost or stolen.

A Card cannot be deleted or cancelled in a Mobile Wallet, however, you may suspend or cancel a Card by contacting Bankwest anytime on 13 17 19.

It may be possible to make EFT Transactions using a Mobile Wallet after deleting or uninstalling the Mobile Wallet application on a mobile device. If a User no longer wishes to use a Card with a Mobile Wallet, the Card should be removed from the Mobile Wallet prior to deleting or uninstalling it on the mobile device. Other ways to ensure that a Card cannot be used with the Mobile Wallet include:

- removing the account the User has with the technology company who issued the Mobile Wallet and to which the Card was added in the relevant Mobile Wallet;
- undertaking a factory reset of the mobile device; and
- erasing the mobile device on the device manager program for the mobile device.

A Card may also be removed from a Mobile Wallet where the mobile device has not connected to Mobile Wallet issuer's servers for at least 90 days.

We will not be liable for any loss caused by a User's fraud or use of a Mobile Wallet or mobile device in a manner not permitted by the issuer of the Mobile Wallet or manufacturer of the mobile device. We will also not be liable for any loss arising from reduced service levels that are outside our reasonable control.

When Bankwest may suspend or terminate a Bankwest Card on a Mobile Wallet

Bankwest may suspend or terminate a Card registered with a Mobile Wallet if:

- you ask us to suspend or cancel the Card;
- a User breaches these terms;
- we, or the issuer of the Mobile Wallet, reasonably suspect fraud or if we are required to do so under anti-money laundering and counter-terrorism financing legislation;

- the issuer of the Mobile Wallet suspends or terminates the Mobile Wallet; or
- we reasonably exercise our discretion to do so, as noted in these Credit Card Account Access Conditions of Use or the Conditions of Use specific to the credit card account.

We will also suspend or terminate the Card when we receive your instructions to do so.

Part 3 - Telephone Banking and Bankwest Online Banking Conditions of Use

3.1 About this Part

This Part (together with Parts 1, 5, 6 and 7) applies to use of Telephone Banking and Bankwest Online Banking in connection with your Facility.

3.2 What is Telephone Banking?

Telephone Banking is a service which enables a user to make enquiries and effect transactions on the Card Account using a PAN and password and tone telephone or mobile phone.

Users must not use an analogue mobile phone as the tone message may be scanned and the PAN and password may be disclosed.

3.3 What can be done using Telephone Banking?

Users of a Business Mastercard can:

- obtain the balance of the Card Account;
- transfer funds between your nominated Bankwest-branded accounts;
- enquire about transactions on the Card Account;
- make payments to the Card Account;
- make bill payments and receive or access bills electronically through the BPAY scheme;
- postdate funds transfer and bill payments up to 90 days in advance; and

- change a password.
- Users of a Corporate Mastercard can:
- obtain the available credit of the Sub Account for their card;
- transfer funds between your nominated Bankwest-branded accounts;
- enquire about transactions on the Sub Account for their card;
- make payments to the Sub Account for their card;
- make bill payments and receive or access bills electronically through the BPAY scheme;
- postdate funds transfer and bill payments up to 90 days in advance; and
- change a password.

Care! Access to the Corporate Mastercard Card Account is not available using Telephone Banking.

3.4 How to use Telephone Banking

To use Telephone Banking users must:

- phone us for the cost of a local call Australia wide. Calls from mobile phones and calls made from overseas are charged at the applicable rate;
- enter their PAN and password using the telephone keypad; and
- follow the instructions given.

3.5 What is Bankwest Online Banking?

Bankwest Online Banking is a service provided by us which enables a user to make enquiries and effect transactions over the Internet on the Card Account using a PAN and password. Bankwest Online Banking must only be accessed via an approved browser.

3.6 What can be done using Bankwest Online Banking?

Users of a Business Mastercard can:

- obtain the balance of the Card Account;
- transfer funds between your nominated Bankwest-branded accounts;

- enquire about transactions on the Card Account;
- check past statements on the Card Account;
- order a printed statement on the Card Account;
- make payments to the Card Account;make bill payments and receive or access bills electronically through the BPAY scheme;
- postdate funds transfer and bill payments;
- change a password;
- lodge various service and application forms with us; and
- make a Pay AnyBody transfer (see Part 4).

Users of a Corporate Mastercard can:

- obtain the available credit of the Card Account for their Sub Account;
- transfer funds between your nominated Bankwest-branded accounts;
- enquire about transactions on the Sub Account for their card;
- check past statements on the Sub Account for their card;
- order a printed statement on the Sub Account for their card;
- make payments to the Sub Account for their card;
- make bill payments and receive or access bills electronically through the BPAY scheme;
- postdate funds transfer and bill payments;
- change a password;
- lodge various service and application forms with us; and
- make a Pay AnyBody transfer (see Part 4).

We provide a version of Bankwest Online Banking that has been customised for mobile devices. Not all of the functions set out in this clause 3.6 will be available when accessing Bankwest Online Banking using a mobile device, and other functions may operate with a reduced level of functionality.

3.7 How to use Bankwest Online Banking

To use Bankwest Online Banking users must have a PAN and password.

The PAN will be provided separately from any password or security token we provide, and upon their receipt, users should visit our website (bankwest.com.au) to get further information and to log on to Bankwest Online Banking.

Users without a Security Token logging onto Bankwest Online Banking for the first time will be required to change their issued password to an alphanumeric code of 8-16 characters and in the form required by us as described in Bankwest Online Banking from time to time. Users with a Security Token logging on for the first time will be required to choose a token PIN.

Where you are registered with SMS Code Security, you must enter your current SMS Code when requested for conducting certain transactions in Bankwest Online Banking.

Where you are registered with Secret Questions Security, you must correctly answer Secret Questions when requested to perform certain transactions or use certain functions in Bankwest Online Banking.

However, SMS Code Security and Secret Questions Security are not available when you conduct transactions or perform functions in Bankwest Online Banking through the version of Bankwest Online Banking that has been specially customised for mobile devices referred to in clause 3.6.

3.8 Internet security and privacy

Users of Bankwest Online Banking must ensure that they take all reasonable steps to protect the security of their electronic equipment, any security token issued to them and their password. This includes, but is not limited to:

- ensuring that, if and when the password is changed, the number and letters which are chosen cannot be easily identified, e.g. it has no obvious pattern (patterns such as 1234A, 1111A, and ABCDEF are too obvious) and has no connection with the user (such as a birthday, telephone number, car registration, postcode or the PIN used with a card);
- ensuring their computer is free of viruses;

- ensuring their computer is not left unattended while they are logged on to Bankwest Online Banking;
- ensuring their computer is free from any form of password recording program or mechanism;
- ensuring that they shut down all browser windows used to gain access to Bankwest Online Banking and that the 'back' function or similar function cannot be used to trace their activities.

The security guidelines in this subclause provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised transactions.

Liability for unauthorised transactions will be determined in accordance with Part 5 of these Account Access Conditions of Use.

3.9 Access and restriction of access to Services

Access to Telephone Banking and/or Bankwest Online Banking may not be available from some States, Territories or country telephone exchanges, or for Bankwest Online Banking, from overseas. You should refer to your telecommunications provider/carrier for information about whether a mobile device will be able to use the relevant overseas network and access Bankwest Online Banking overseas.

We will try (without any legal obligation) to provide the Services on a 24-hour continuous basis. However, circumstances may not always make this possible.

If the Services cannot be accessed at any time, to help us to investigate the reason please advise us by calling us.

Subject to clause 6.4, we are not responsible for:

- the inability of any computer or mobile device to access or use Bankwest Online Banking. You are responsible for compatibility of any computer or mobile device with Bankwest Online Banking;
- the unavailability of Bankwest Online Banking as a result of the failure of any telecommunication connection used in connection with a computer or mobile device; or
- any loss or damage to any computer or mobile device as a result of the use or attempted use of Bankwest Online Banking.

You are responsible for any fees or charges imposed by a telecommunications provider/carrier for accessing Telephone Banking or Bankwest Online Banking, including call costs and costs for accessing the Internet where you access Bankwest Online Banking using a mobile device, whether Bankwest Online Banking is accessed from Australia or overseas. You should refer to your telecommunications provider/carrier for full details about the fees and charges associated with accessing and downloading information from the Internet.

We do not guarantee to give effect to any payment instruction received via our Services. We may delay and/or refuse to give effect to any Telephone Banking or Bankwest Online Banking instruction without notifying you. Instructions will not be processed:

- when your Facility prohibits the payment(s);
- when the limit of the Card Account or Facility would be exceeded;
- when any individual Card limit would be exceeded; or
- when a BPAY payment will cause you to exceed your daily BPAY payment limit.

Users should ensure that any transaction instruction they give would not cause the Facility limit to be exceeded.

Except for BPAY and Pay AnyBody transactions, transactions made prior to 6.00 pm WST on a business day should be processed that day and otherwise should be processed on the next business day. However, payments to credit card accounts will not be available until the day after the next business day.

3.10 Future payments

If a funds transfer, BPAY payment or Pay AnyBody transfer is scheduled for a future stipulated date, it will only be effected on that date by us if the payment will not cause your limit applicable to the Card Account to be exceeded by 11.30pm WST on the business day prior to the scheduled payment date and the funds transfer, BPAY payment or Pay AnyBody transfer will not cause you to exceed any limit we impose in accordance with clause 3.11, your daily BPAY payment limit or your daily Pay AnyBody transfer limit on the date stipulated for the payment to be made.

3.11 Limits

At our discretion we may impose and/or vary minimum and/or maximum limits on the amounts which users may transfer from the Card Account using our Services.

Current information on these limits can be accessed by logging in to Bankwest Online Banking and selecting the "payments and transfers" menu, then selecting "payment limits" or by calling the Business Customer Relationship Centre on **13 70 00**.

3.12 Other matters

We shall issue a receipt number for each funds transfer or BPAY payment instruction received via our Services.

When we have instructions for more than one transfer or BPAY payment from the Card Account we may determine the order of priority in which the transfers or payments are made. In making any such determination, we will act reasonably.

3.13 Authorised users

Each Cardholder will have automatic access to our Services with their own PAN and password.

3.14 BPAY Payments

(a) If there is any inconsistency between the provisions of this clause 3.14 and any other provision of these Account Access Conditions of Use, this clause 3.14 prevails to the extent of that inconsistency.

(b) When a user tells us to make a BPAY payment, they must give us the information specified in paragraph (f) below. We will then debit the Card Account with the amount of that BPAY payment.

(c) All bill payments that are made through our Services are processed through the BPAY scheme. Bills which may be paid through the scheme display the BPAY logo and Biller reference details. The bill will also record the type of accounts the Biller will accept payment from (e.g. cheque, savings, or credit card).

(d) Telephone Banking users may nominate a maximum of 12 BPAY Billers per PAN on their frequent Billers list. Bankwest Online Banking users may nominate a maximum of 500 BPAY Billers on their frequent Billers

list, with the first 12 BPAY Billers stored in the frequent Billers list also available in Telephone Banking. Users will be able to pay other BPAY Billers by manually keying in their full details.

(e) The initial maximum aggregate amount of BPay payments that you may instruct us to make on any business day is $5,000. Higher limits may be arranged online after registering for SMS Code Security or Secret Questions Security.

Higher limits may also be arranged by calling the Business Customer Relationship Centre on 13 70 00. Approval is subject to our sole discretion.

Different limits may apply for the version of Bankwest Online Banking that has been specially customised for mobile devices referred to in clause 3.6.

Current information on these limits can be accessed by logging in to Bankwest Online Banking and selecting the "payments and transfers" menu, then selecting "payment limits" or by calling the Business Customer Relationship Centre on 13 70 00.

Certain transactions may require SMS Code Security or Secret Questions Security at lower limits as determined by us from time to time.

(f) The following information must be given to us to make a BPAY payment:

i. the Biller code;

ii. the Biller customer reference number;

iii. the amount to pay;

iv. a date if the payment is to be postdated; and

v. the account to be debited for the payment.

(g) We shall not be obliged to effect a BPAY payment instruction if the information is incomplete and/or inaccurate, the payment would cause the limit of the Card Account or the daily BPAY payment limit to be exceeded.

(h) A BPAY payment from the Card Account is treated as a purchase transaction.

(i) Except for postdated payments (clause 3.14(n)) we will not accept an order to stop a BPAY payment once we have been instructed to make the BPAY payment.

(j) Generally, a BPAY payment will be treated as received by the Biller to whom it is directed:

i. on the date we are told to make that BPAY payment, if we receive the instruction before 4.00 pm WST on a business day; or

ii. on the next business day, if we receive the instruction after 4.00 pm WST on a business day, or on a non-business day.

(k) A delay may occur in processing a BPAY payment where a Biller, or another financial institution participating in the BPAY scheme, does not comply with its obligations under the BPAY scheme.

(l) Care must be taken by all users to enter the correct amount to be paid to a Biller and to enter the correct Biller details. If the amount entered is greater than was intended, you must contact the Biller to obtain a refund of the excess. If less, a further BPAY payment can be made. If the payment is made to a person other than the Biller intended to be paid and we cannot recover it from the recipient within 20 business days, you are liable for the amount.

(m) If we are advised that a BPAY payment cannot be processed by a Biller, we will advise you, credit the Card Account with the amount of the BPAY payment, and take all reasonable steps to assist in making the BPAY payment as quickly as possible.

(n) Postdated BPAY payments:

i. A BPAY payment may be requested for a date in the future, however, we will only make the BPAY payment if the requirements of clause 3.10 are met. If the date stipulated is not a business day, we will make the BPAY payment on the next business day. In the event that the Facility limit, your daily BPAY payment limit, any individual Card limit or any other limit we impose in accordance with clause 3.11 is exceeded, it will be necessary to re-submit the BPAY payment instruction.

ii. A future-dated BPAY payment instruction may be altered or cancelled before its stipulated date for payment, provided the instruction to alter or cancel the payment is given before the payment cut-off time the business day immediately prior to the stipulated date.

(o) We may charge a fee to correct errors on the Card Account due to incorrect BPAY instructions.

(p) You acknowledge that the receipt by a Biller of a mistaken or erroneous payment does not or will not constitute under any circumstances part or whole satisfaction of any underlying debt owed between you and that Biller.

(q) You should check the Card Account carefully and promptly report to us, as soon as you become aware of them, any BPAY payments that you think are errors or are BPAY payments that you did not authorise. (NOTE: The longer the delay between the date of your BPAY payment and when you tell us of the error, the more difficult it may be to correct the error. For example, we or your Biller may not have sufficient records or information available to us to investigate the error. If this is the case you may need to demonstrate that an error has occurred, based on your own records, or liaise directly with the Biller to correct the error.)

(r) Your liability for unauthorised and fraudulent BPAY payments will be determined in accordance with Part 6 of these Account Access Conditions of Use.

(s) Disputes in relation to unauthorised, fraudulent or wrong BPAY payments will be handled in accordance with Part 7 of these Account Access Conditions of Use, however, no chargeback rights are available in respect of a BPAY payment from the Card Account.

(t) If a BPAY payment is made to a person or for an amount which is not in accordance with the instructions given to us and the Card Account was debited with the payment, we will credit that payment amount to your account.

(u) If you tell us that a BPAY payment made from the Card Account is unauthorised, you must give us your written consent addressed to the Biller who received that BPAY payment, consenting to us obtaining from the Biller information about your account with that Biller or the BPAY payment, including your customer reference number and such information as we reasonably require to investigate the BPAY payment. If you do not give us that consent, the Biller may not be permitted under law to disclose to us the information we need to investigate or rectify that BPAY payment.

(v) Subject to Part 6 of these Account Access Conditions of Use:

i. we are not liable for any consequential loss or damage you may suffer as a result of using the BPAY scheme, other than due to any loss or damage you suffer due to our negligence, or in relation to any breach of a condition or warranty implied by law in contracts for the supply of goods and services and which may not be excluded, restricted or modified at all or only to a limited extent; and

ii. you indemnify us against any loss or damage we may suffer due to any claim, demand or action of any kind brought against us arising directly or indirectly because you:

- did not observe any of your obligations under; or
- acted negligently or fraudulently in connection with, this clause 3.14.

3.15 BPAY View

(a) Users may use BPAY View to receive or access bills electronically from participating Billers nominated by you. A user can access a bill by accessing Bankwest Online Banking.

(b) You need to register and individual users need to register in order to use BPAY View. Call us on 13 70 00 to find out how to register, or register online via Bankwest Online Banking.

(c) If you or a user registers with BPAY View, they:

i. agree to our disclosing to Billers nominated by you:

- such of your personal information (for example your name, email address and the fact that you are our customer) as is necessary to enable Billers to verify that you can receive bills and statements electronically using BPAY View (or telling them if you cease to do so); and
- that an event in paragraph (d)(ii), (iii), (iv), (v) or (vi) has occurred;

ii. agree to us or a Biller (as appropriate) collecting data about whether you access your emails, the Bankwest Online Banking website and any link to a bill or statement;

iii. agree to receive bills and statements electronically and agree that this satisfies the legal obligations (if

any) of a Biller to give you bills and statements. For the purposes of this clause we are the agent for each Biller nominated by you under (i) above.

(d) You may receive paper bills and statements from a Biller instead of electronic bills and statements:

i. at your request to a Biller (a fee may be charged by the applicable Biller for supplying the paper bill or statement to you if you ask for this in addition to an electronic form);

ii. if you or a Biller de-register from BPAY View;

iii. if we receive notification that your email mailbox is full, so that you cannot receive any email notification of a bill or statement;

iv. if your email address is incorrect or cannot be found and your email is returned to us undelivered;

v. if we are aware that you are unable to access your email or Bankwest Online Banking or a link to a bill or statement for any reason; or

vi. if any function necessary to facilitate BPAY View malfunctions or is not available for any reason for longer than the period specified by the applicable Biller.

(e) You agree that when using BPAY View:

i. If you receive an email notifying you that you have a bill or statement, then that bill or statement is received by you:

- when we receive confirmation that your server has received the email notification, whether or not you choose to access your email; and
- at the email address nominated by you;

ii. if you receive notification via Bankwest Online Banking without an email then that bill or statement is received by you:

- when a notification is posted on Bankwest Online Banking, whether or not you choose to access Bankwest Online Banking; and
- via Bankwest Online Banking;

iii. bills and statements delivered to you remain accessible through Bankwest Online Banking for the period determined by the Biller up to a maximum of 18 months, after which they will be deleted, whether paid or not;

iv. you will contact the Biller directly if you have any queries in relation to bills or statements.

(f) You must:

i. check your emails or log onto Bankwest Online Banking at least weekly;

ii. tell us if your contact details (including email address) change;

iii. tell us if you are unable to access your email or log onto Bankwest Online Banking or a link to a bill or statement for any reason; and

iv. ensure your mailbox can receive email notifications (e.g. it has sufficient storage space available).

(g) BPAY View billing errors

i. For the purposes of this paragraph (g) a BPAY View billing error means any of the following: If you have successfully registered with BPAY View:

- failure to give you a bill (other than because you failed to view an available bill);
- failure to give you a bill on time (other than because you failed to view an available bill on time);
- giving a bill to the wrong person;
- giving a bill with incorrect details;
- If your BPAY View deregistration has failed for any reason:
- giving you a bill if you have unsuccessfully attempted to deregister from BPAY View.

ii. You agree that if a billing error occurs:

- you must immediately upon becoming aware of the billing error take all reasonable steps to minimise any loss or damage caused by the billing error, including contacting the applicable Biller and obtaining a correct copy of the bill; and
- the party who caused the error is responsible for correcting it and paying any charges or interest which would ordinarily be payable to the applicable Biller due to any consequential late payment and as a result of the billing error.

iii. You agree that for the purposes of this paragraph (g) you are responsible for a billing error if the billing error occurs as a result of an act or omission by you

or the malfunction, failure or incompatibility of computer equipment you are using at any time to participate in BPAY View.

Part 4 - Pay Anybody Conditions of Use

4.1 About these conditions

Part 4 (together with Parts 1, 5, 6 and 7) of these Conditions of Use applies to all transactions involving the use of the Bankwest Online Banking Pay AnyBody Service (Pay AnyBody). The Pay AnyBody Conditions of Use operate in conjunction with the Conditions of Use applicable to Bankwest Online Banking (see Part 3 above) and to your nominated accounts accessed using these services. The Pay AnyBody Conditions of Use prevail to the extent of any inconsistency.

4.2 What is Pay AnyBody?

Pay AnyBody is a service which allows a user to transfer funds from a nominated Bankwest-branded account to:

another account (except a credit card account) held by you with another financial institution; or

another person's account (except a credit card account) held with us or with another financial institution.

Except non-Bankwest-branded credit card accounts.

4.3 Daily Pay AnyBody transfer limit

The initial maximum aggregate amount of Pay Anybody payments that you may instruct us to make on any business day is $1,500. Higher limits may be arranged online after registering for SMS Code Security or Secret Questions Security.

Higher limits may also be arranged by calling Business Customer Relationship Centre on 13 70 00. Approval is subject to our sole discretion.

Different limits may apply for the version of Bankwest Online Banking that has been specially customised for mobile devices referred to in clause 3.6.

Current information on these limits can be accessed by logging in to Bankwest Online Banking and selecting the

"payments and transfers" menu, then selecting "payment limits" or by calling the Business Customer Relationship Centre on **13 70 00**.

Certain transactions may require SMS Code Security or Secret Questions Security at lower limits as determined by us from time to time.

4.4 Making a Pay AnyBody transfer

(a) The following information must be given to us to make a Pay AnyBody transfer in respect of the account to which the funds are to be transferred:

- the BSB number;
- the account number; and
- the account name; and
- a description of the transaction.

(b) We shall not be obliged to effect a Pay AnyBody transfer if the information is incomplete and/or inaccurate, there is a technical failure which prevents us from processing the transfer, the transfer would cause the limit of the Card Account, any individual Card limit or your daily Pay AnyBody transfer limit to be exceeded.

(c) A Pay AnyBody transfer from the Card Account is treated as a cash advance.

4.5 Postdated Pay AnyBody transfers

(a) A Pay AnyBody transfer may be requested for a date in the future, however, we will only make the Pay AnyBody transfer if the requirements of clause 3.10 are met. If the date stipulated is not a business day, we will make the Pay AnyBody transfer on the next business day.

(b) A future-dated Pay AnyBody transfer may be altered or cancelled before its stipulated date provided the instruction to alter or cancel the transfer is given before 11.30pm WST on the business day immediately prior to the stipulated date.

4.6 Cancelling a Pay AnyBody transfer

We are not obliged to cancel a Pay AnyBody transfer once we have accepted the instruction to make it. It may be

possible in some cases to cancel an initiated Pay Anybody transfer. A fee may be payable for any such cancellation.

4.7 Mistakes as to the amount of a Pay AnyBody transfer

Care must be taken by all users to enter the correct amount to be transferred. If the amount entered is greater than was intended you should seek a refund from the recipient. If less, a further transfer can be made.

4.8 Processing Pay AnyBody transfers

(a) Our payment cut-off time for a Pay AnyBody transfer to be effected to another Bankwest-branded account on the same day is 2.00pm WST.

(b) Generally, a Pay AnyBody transfer will be treated as received by another financial institution or in relation to a non-Bankwest-branded account:

- on the date we are told to make that Pay AnyBody transfer, if we receive the instruction before 2.00pm WST on a business day; or
- on the next business day, if we receive the instructions after 2.00pm WST on a business day, or on a non-business day.

(c) A delay may occur in processing a Pay AnyBody transfer where:

- we need to verify that the transaction is an authorised transaction;
- there is a public holiday on the day or the day we are told to make a Pay AnyBody transfer; or
- another financial institution participating in the Pay AnyBody transfer scheme does not comply with its obligations under that scheme.

(d) If we are advised that a Pay AnyBody transfer cannot be processed by another financial institution, we will:

- advise you of this;
- credit the Card Account with the amount of the Pay AnyBody transfer; and
- take all reasonable steps to assist in making the Pay AnyBody transfer as quickly as possible.

4.9 Liability for unauthorised transactions and fraud

Your liability for unauthorised and fraudulent transactions will be determined in accordance with Part 7.

4.10 Liability for mistaken payments

If a Pay AnyBody transfer is made to a person or for an amount, which is not in accordance with the instructions (if any) given to us, and the Card Account was debited for the amount of that payment, we will credit that payment to your account. However, if you are responsible for a mistake resulting in that payment and we cannot recover the amount of that payment from the person who received it, you must pay us that amount.

Part 5 - Security of Access Methods

5.1 What do users need to do to safeguard their access methods?

Users must protect relevant access methods to prevent unauthorised access to their Card Account. Users must take care to ensure that access methods are not misused, lost or stolen and that secret codes do not become known to anyone else.

5.2 Guidelines

This clause contains guidelines which should be followed by users to guard against unauthorised use of an access method. These guidelines provide examples only of security measures and will not determine your liability for losses resulting from any unauthorised transactions.

Liability for unauthorised transactions will be determined in accordance with Part 6 of these Commercial Cards Account Access Conditions of Use.

To protect a Card the user must:

- sign the Card as soon as it is received;
- carry the Card with them whenever possible;
- always keep the Card in a safe, secure place and check regularly to ensure it has not been lost or

stolen;

- never give the Card to anybody or permit any other person to use the Card or Card details, including family and friends; and
- when the transaction is complete remember to take the Card and the transaction receipt.

To protect the Card details the user must:

- not give or tell the Card details to anyone; and
- use care to prevent anyone seeing the Card details when entering them at electronic equipment

To protect the secret code:

- the user must, where the secret code is issued by us, memorise the secret code when it is received. Once memorised, destroy our notice of the secret code. If a user forgets the secret code they may apply to us for it to be reissued;
- if given the option to select a secret code, users should not select a secret code which represents a name, date, telephone number, car registration or anything else that could be associated with them, or select a secret code which has an easily retrievable combination (such as repeated numbers or letters);
- never tell or show a secret code to anyone, including a family member, friend or persons in authority (such as a bank officer or police officer);
- do not record a secret code on the Card and/or Security Token;
- do not record the secret code on anything which is kept with or near the Card or Security Token without making a reasonable attempt to disguise the secret code;
- do not keep a record of the secret code (without making any reasonable attempt to disguise the secret code) with any article kept with the Card or Security Token which is liable to be lost or stolen simultaneously with the Card;
- do not record the secret code on a computer or telephone or related articles without making a reasonable attempt to disguise the secret code or prevent unauthorised access to the records;
- do not keep the Card or Security Token and a secret code together, for example in a bag or wallet, in a car or in the same piece of furniture;
- do not keep a record of the secret code with any document containing the reference numbers for the Card Account, such as statements;
- if a user selects their own secret code, for security

reasons it should be changed at regular intervals, e.g. every two years; and

- if a user suspects that someone else may know a secret code or that an unauthorised person is using a secret code, they should contact us immediately to request the issue of a new secret code.

We do not consider the following to be reasonable attempts to disguise a secret code:

- recording the disguised secret code on their Card;
- disguising the secret code by reversing the number sequence;
- describing the disguised record as a secret code record;
- disguising the secret code as a telephone number where no other numbers are recorded;
- disguising the secret code as a telephone number, postcode, amount or date with the secret code in its correct sequence within the number;
- disguising the secret code using alphabetical characters, i.e. A=1, B=2, C=3 etc. or in any other easily understood code; or
- recording the secret code as a series of numbers or letters with any of them marked to indicate the secret code.

Users must not use any other forms of disguise which are similarly unsuitable because another person can easily work out the secret code.

At electronic equipment a user must:

- be careful to prevent anyone else from seeing the secret code being entered;
- watch out for mirrors, security cameras or any means which enable other people to see the secret code being entered;
- when the transaction is complete remember to take the Card, transaction receipt and any cash; and
- not access Telephone Banking or Bankwest Online Banking directly from a facility where the details entered may be recorded by a third party, e.g. a hotel telephone or a computer at an internet cafe.

To protect the Security Token a user must:

- carry the Security Token with them whenever possible;
- always keep the Security Token in a safe, secure place and check regularly to ensure it has not been lost or stolen;

- not record account numbers, their PAN, or secret code details on the Security Token;
- not drop the Security Token or expose it to high heat, water or attempt to dissemble it;
- not keep the Security Token with any document containing the reference numbers for Nominated Accounts or with other account information such as statements or cheque books;
- not lend the Security Token to anyone, or permit anyone to use the Security Token.

To protect the security of a Mobile Wallet:

(a) where a mobile device can be accessed by a Biometric Identifier, the user you should ensure only the user's Biometric Identifier is registered on the mobile device;

(b) where the mobile device is accessible by a secret code, the secret code must be kept secure by the user. It must not be disclosed to anyone else (even a family member), a record of the secret code must not be kept with the mobile device, or with or in anything with which the mobile device is stored unless reasonable steps have been taken to protect it;

(c) any secret code selected must not be easy to guess or decipher, such as a user's date of birth or other number associated with the user;

(d) a user must not act with extreme carelessness in relation to the security of the secret code;

(e) a user must ensure the mobile device is locked at all times when it is not being used, and is not left unattended in a non-secure environment;

(f) a user must install and regularly update anti-virus software on the mobile device;

(g) a user must ensure that only the user accesses the Mobile Wallet to use the user's Card and that it is not accessed or used by anyone else, even if that person has the user's permission; and

(h) a user must remove any Card from the user's mobile device before disposing of the mobile device.

Biometric identifiers and Secret Codes

If another person's Biometric Identifier is loaded onto a user's mobile device, you must ensure that the relevant user takes immediate steps to remove the Biometric

Identifier from the relevant mobile device, otherwise any transaction using that Biometric Identifier will not be an unauthorised transaction for the purposes of determining liability.

Reporting security concerns to Bankwest

You must notify Bankwest immediately if:

(a) a user's mobile device is disconnected without the knowledge or permission of the user;

(b) you or any user suspects that someone has used the mobile device or a secret code to conduct an EFT Transaction or otherwise tried to access the mobile device or Mobile Wallet.

5.3 Financial Crimes Monitoring

In order for us to meet our regulatory and compliance obligations for anti-money laundering and counter financing of terrorism, we will be increasing the levels of control and monitoring we perform. You and users should be aware that:

- transactions may be delayed, blocked or refused where we have reasonable grounds to believe that they breach Australian law or the law of any other country;
- we may from time to time require additional information from you or other users to assist us in the above compliance process;
- where legally obliged to do so, we may disclose the information gathered to regulatory and/or law enforcement agencies.

You must not, and users must not, initiate or conduct a transaction that may be in breach of Australian law or the law of any other country.

Part 6 - Loss, Theft or Unauthorised Use of an Access Method

6.1 What users have to do

If:

- any Card;
- PIN;
- Security Token; or
- mobile device on which a Card has been loaded using a Mobile Wallet,

has been lost, stolen or used without authorisation, or a secret code has become known to someone else, you or any Cardholder must immediately tell us or, in the case of a Card, tell any bank displaying the Mastercard symbol, in writing or by calling us.

We will require all information about how the loss, theft or unauthorised use occurred.

We will issue a notification number which should be kept as evidence of the date and time of the notification.

If a Card is lost or stolen in Australia or overseas, the best way to contact us is by telephone so that we can immediately place a stop on the Card.

If a Card is lost or stolen overseas, you or the Cardholder may report the loss to:

- Mastercard Global Service; or
- Any financial institution displaying the Mastercard scheme sign.

If for any reason the emergency telephone facility is unavailable and this prevents the user from calling us you will not be liable for any unauthorised transactions which could have been prevented during this period if the user had been able to telephone us. However, the user must notify us within a reasonable time of the emergency facility becoming available again.

6.2 What is your liability for unauthorised EFT Transactions?

You are liable for all EFT Transactions carried out in respect of the Card Account with the knowledge and

consent of a user except where a Mobile Wallet is used. Part 6A deals with liability for transactions made using a Mobile Wallet.

6.2.1 When you are not liable

You will not be liable for any unauthorised EFT transactions that occur:

- using a Card or Card details, Security Token or secret code before the user has received their Card, Security Token or secret code (as relevant);
- in connection with a Card, Payment Device or security token (as relevant) after we receive notification of the misuse, loss or theft or the secret code becoming known to someone else;
- relating to any component of an access method that is forged, faulty, expired or cancelled;
- by the fraudulent or negligent conduct of our employees or agents, or the employees or agents of merchants or of companies or persons involved in the EFT system;
- where it is clear that the user has not contributed to the loss; or
- due to the same transaction being incorrectly debited more than once to the Card Account.

6.2.2 When you are liable

Where we prove on the balance of probabilities that a user has contributed to losses in respect of the Card Account resulting from an unauthorised EFT transaction by:

- the user's fraud;
- (in all cases except where the unauthorised EFT transaction was made using Bankwest Online Banking and the user has been issued with a Security Token) voluntarily disclosing the secret code to anyone, including a family member or friend;
- (where the unauthorised EFT transaction was made using Bankwest Online Banking and the user has been issued with a Security Token) voluntarily disclosing the token PIN and showing the Security Token or otherwise disclosing the token code to anyone, including a family member or friend;

- (where the unauthorised EFT transaction was made using Bankwest Online Banking and the user has been issued with a Security Token), either:
  - voluntarily disclosing the token PIN; or
  - showing the Security Token (or otherwise disclosing the token code), to anyone, including a family member or friend, where this disclosure is more than 50% responsible for the losses when all contributing causes are assessed together;
- (in all cases except where the unauthorised EFT Transaction was made using Bankwest Online Banking and the user has been issued with a Security Token), indicating a secret code on the Card, or keeping a record of a secret code (without making any reasonable attempt to protect the security of the record) on the one article, or on several articles, carried with the Card or liable to loss or theft simultaneously with the Card;
- (where the unauthorised EFT Transaction was made using Bankwest Online Banking and the user has been issued with a Security Token) indicating the token PIN on the Security Token, or keeping a record of the token PIN (without making any reasonable attempt to protect the security of the code record) on the one article, or on several articles, carried with the security token or liable to loss or theft simultaneously with the Security Token;
- where the access method comprises a secret code without a Card or Security Token, keeping a record of a secret code (without making any reasonable attempt to protect the security of the code records) on the one article, or on several articles that are liable to loss or theft simultaneously;
- when changing a secret code, selecting a secret code which represents the user's birth date or a recognisable part of the user's name;
- acting with extreme carelessness in failing to protect the security of the secret code; or
- leaving a card in an ATM, as long as the machine incorporates reasonable safety standards that mitigate the risk of a card being left in the machine (for example, the machine captures cards that are not removed after a reasonable time or requires that the card be removed from the machine before the transaction can proceed)

You will be liable for the losses which occur before we are notified of the unauthorised use, loss or theft of the

Card or Security Token, or breach of the security of the secret code; or by:

- where we prove on the balance of probabilities that a user has contributed to a loss resulting from an unauthorised EFT Transaction by unreasonably delaying in notifying us of the unauthorised use, theft or loss of the Card or Security Token, or that the secret code has become known to someone else

You will be liable for the losses which occur between when the user became aware of the loss, theft or unauthorised use (or should reasonably have become aware in the case of a lost or stolen Card or Security Token) and when we were actually notified.

However, in all cases you will not be liable for:

(a) that portion of the loss incurred on any one day which exceeds any applicable daily transaction limits;

(b) that portion of the loss incurred in a period which exceeds any other periodic transaction limit applicable to that period;

(c) losses incurred on any accounts which you had not agreed with us could be accessed using the access method;

(d) losses that would exceed the amount of your liability had we exercised our rights (if any) under the Credit Card scheme rules against other parties to that scheme; or

(e) that portion of the loss which exceeds the limit of the Card Account.

6.2.3 When your liability is limited

Where a secret code was required to perform the unauthorised EFT Transaction and clause 6.2.2 does not apply, your liability for any loss in respect of the Card Account arising from an unauthorised EFT Transaction, if the loss occurs before we are notified of the unauthorised use, loss or theft of the Card or Security Token or the password becoming known to someone else, is lesser of:

- $150;
- the actual loss at the time we are notified of the unauthorised use, loss or theft of the Card or Security Token or of the secret code becoming known to someone else (except that portion of the loss that exceeds any daily or periodic transaction

limits applicable to the use of your access method or Card Account);

- the limit of the Card Account; or
- the amount of your liability had we exercised our rights (if any) under the Credit Card scheme rules against other parties to the scheme.

6.3 What is your liability for other unauthorised transactions?

If, in cases not involving EFT Transactions, a Card is used without a user's authority, you are liable for the actual loss arising from the transaction at the time we are notified of the unauthorised use (except that portion of the loss incurred on any one day that exceeds any applicable daily transaction or other periodic transaction limit) less any amount recovered by us in the exercise of our rights (if any) under the Credit Card scheme rules against other parties to that scheme.

6.4 When the electronic banking system or EFT terminal malfunctions or breaks down

In the event that an EFT terminal malfunctions or breaks down, manual procedures may be available from the merchant for retail transactions by using the Card and a signature authorisation procedure.

You will not be responsible for any loss you suffer because our system or our equipment accepted a user's instructions but failed to complete the transaction.

If the users were or acting reasonably should have been aware that the EFT system or equipment was unavailable for use or malfunctioning then our liability is limited to correcting any errors in the Card Account and the refund of any charges or fees imposed on you as a result. We will not be responsible if an EFT terminal does not accept your instructions or the Card fails to work in the terminal.

Please advise us if an EFT terminal has a service fault or difficulty. Users can do this through our Customer Support Team during normal banking hours or by telephoning us.

Part 6A - Liability For Mobile Wallet Transactions

6A.1 Application of this Part

This Part deals with liability for EFT Transactions which are carried out using a Mobile Wallet and a mobile device.

6A.2 Authorised transactions

You are liable for all EFT Transactions carried out in respect of your Card Account with a user's mobile device and a Mobile Wallet including:

- EFT Transactions carried out in respect of your Card Account with the knowledge and consent of a user; and
- EFT Transactions which were able to be carried out as a result of a failure to comply with the security measures described for mobile devices and Mobile Wallets in clause 5.2.

6A.3 When you are not liable for EFT transactions made using a Mobile Wallet

You will not be liable for losses in respect of a Card Account caused by an EFT Transaction made using a Mobile Wallet:

(a) resulting from unauthorised use of a Card before the User has received the Card;

(b) in connection with a Card, after we receive notification of the misuse, loss or theft or the secret code becoming known to someone else;

(c) caused by the fraudulent or negligent conduct of employees or agents of:

- us;
- any organisation involved in the provision of the EFT system; or
- any Merchant;

(e) where it is clear that the User has complied with all of the security measures described for mobile devices and Mobile Wallets in clause 6.2; or

(f) caused by the same EFT Transaction being incorrectly debited more than once to the same account.

Part 7 - Procedures for Handling Errors and Disputed Transactions

7.1 How will any errors, mistakes and disputes be handled?

If you believe an entry on your statement of account is wrong or unauthorised you must tell us immediately by:

- telephoning us on **13 70 00**;
- logging on to our website (bankwest.com.au) and following the procedures it sets out for disputing a transaction;
- calling into any of our Customer Service Centres; or
- writing to us at the address shown on your statement of account containing the suspected error.

You must promptly complete a Bankwest Credit Card Transaction Dispute. This form can be obtained from any Customer Service Centre, our website or by calling us.

To assist in the dispute resolution process, you will need to provide the following information:

- the Cardholder's name, address and credit card number;
- details and amount of the transaction, charge, refund or payment in question; and
- supporting documentation (examples being: credit card receipt, delivery advice).

We will notify you of the name and contact number of the officer investigating your dispute.

We have the right under the Credit Card scheme rules to seek the reversal of a credit card transaction, involving a 'chargeback' or debiting of the credit card transaction to the merchant's account with its financial institution including for recurring payment arrangements with a merchant.

We may do so on certain grounds, for instance if you claim that an unauthorised transaction debited to your account was incorrectly charged, and you or any Cardholder did not contribute to the loss.

We will claim a chargeback right where one exists under the Credit Card scheme rules. Please note, however, that no chargeback right will exist in relation to BPAY payments from the Card Account (see clause3.14(s)).

We will use our best efforts to chargeback a disputed transaction for the most appropriate reason. This does not mean that the disputed transaction will necessarily be charged back. The merchant's financial institution must first accept the claim in order for your claim to be successful. If the merchant's financial institution rejects a chargeback, we will not accept that rejection unless we are satisfied that the rejection is reasonable and is consistent with the Credit Card scheme rules.

You should make every effort to report a disputed transaction by completing the Bankwest Credit Card Transaction Dispute Form within 14 days of the date of the statement of account which itemises the disputed transaction, so that we may reasonably ask for a chargeback where such right exists.

Failure to report a disputed transaction, charge, refund or payment, and/or provide additional information within this timeframe could affect our ability to claim a chargeback right (if any) under the Credit Card scheme rules.

These rules all impose time limits on reporting disputed transactions, charges, refunds or payments.

7.1.1 If we are unable to resolve the matter immediately to both your and our satisfaction we will advise you in writing of our procedures for further investigation and handling of your complaint.

7.1.2 Within 21 days of receiving your complaint, we will advise you in writing of either:

- the outcome of our investigation; or
- the fact that we need more time to complete our investigation.
- We will complete our investigation within 45 days of receipt of your complaint unless there are exceptional circumstances.

7.1.3 Subject to clause 7.1.4, if we are unable to resolve your complaint within 45 days we will write to you and let you know the reasons for the delay and provide you with monthly updates on the progress of our investigation

and its likely resolution date, except where we are waiting for a response from you and you have been advised that we require such a response.

7.1.4 If we resolve your complaint by exercising our rights under the Credit Card scheme rules we will:

- apply the time limits under those rules to clause 7.1.2;
- comply with clause 7.1.3 as if the reference to '45 days' read '60 days' and the reference to 'monthly updates' read 'updates every two months';
- inform you when you can reasonably expect a decision; and
- suspend your obligation to pay any amount which is the subject of your complaint or any credit or other charges related to that amount until your complaint has been resolved.

7.2 Outcome

On completion of our investigation, we will advise you in writing of the outcome of our investigation and the reasons for our decision, with reference to the relevant provisions of these Commercial Cards Account Access Conditions of Use. If we decide that the Card Account has been incorrectly charged or credited, we will adjust your account (including any interest and charges) and notify you in writing of the amount of the adjustment. If we decide that you are liable for all or any part of the disputed transaction, we will supply you with copies of any document or other evidence on which we base our findings if these show that the Card Account has not been incorrectly charged or credited. We will also advise you if there was any system or equipment malfunction at the time of the transaction.

We will advise you in writing that, if you are not satisfied with our findings, you may request a review.

7.3 If you are not satisfied

If you are not satisfied with our findings, you may request our Customer Care Department to review the matter.

Contact them by writing to:

Manager Customer Care

GPO Box E237

Perth WA 6841

or phone or fax to:

Telephone: Freecall 1300 259 233

Facsimile: (08) 9449 2555.

When we advise you of our decision we will also advise you of further action you may take in respect of your complaint if you are not satisfied with our decision. For instance, you may be able to refer the matter (free of charge) to:

Australian Financial Complaints Authority Limited

GPO Box 3 Melbourne, VIC 3001

Fax: (03) 9613 6399

Telephone: 1800 931 678

website: www.afca.org.au

You may also be able to refer your complaint to consumer affairs departments or small claims tribunals.

This page has been left blank intentionally

This page has been left blank intentionally

visit any branch
13 7000
bankwest.com.au/business

bankwest

FOR BUSINESS