bankwest

Account Access.

Conditions of Use

Credit Cards

About these Conditions of Use

These Credit Card Account Access Conditions of Use apply to your use of a credit card, a Virtual Card, a Payment Device, Bankwest Online Banking, Phone Banking, and Pay AnyBody to access a credit card account in circumstances where we tell you that these Credit Card Account Access Conditions of Use form part of the credit card contract between us.

This document does not contain all of the information we are required to give you before entering into a credit contract.

Other information is contained in the Credit Card Schedule and the Credit Card Conditions of Use. Each of these Services provides you with access to Bankwest credit card accounts which we agree you may nominate.

You must read these Credit Card Account Access Conditions of Use together with the Credit Card Schedule and the Conditions of Use specific to the credit card account. All three documents comprise your credit card contract. If there is an inconsistency between these Credit Card Account Access Conditions of Use, and the Conditions of Use specific to the credit card account, these Credit Card Account Access Conditions of Use prevail in respect of EFT transactions.

Mobile Wallets with which you 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.

If you wish to use the Bankwest website, or access Bankwest Online Banking via the Bankwest App, the “Website Terms of Use” (available at bankwest.com.au) will also apply.

Customer enquiries

Please call **13 17 19**, message us in the Bankwest App or visit **bankwest.com.au**.

Where to report lost or stolen cards or suspected unauthorised transactions (24 hours):

Through the Bankwest App or Online Banking, including by messaging us.

Within Australia **13 17 19** (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).

Please note that a Mistaken Internet Payment and certain payments made using a Mobile Wallet are not the same as an unauthorised transaction. For Mistaken Internet Payments, refer to clause 4.10 and for payments made using a Mobile Wallet authorised by Biometric Identifiers refer to clause 6.2.

Information on standard fees, charges and any interest rates is available on request.

Contents

Part 1 – General

1.1 Definitions

In addition to the definitions in the Bankwest Credit Card Conditions of Use, the following definitions apply to this document:

Access Method means a method 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, a Payment Device 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.

ADI means any bank, building society, credit union or other authorised deposit-taking institution within the meaning of the Banking Act 1959 (Cth).

Approved Browser means a browser which can be used to access Bankwest Online 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.

Biometric Identifier means a unique biometric trait, including without limitation, a fingerprint, facial recognition, voice recognition, body feature recognition, 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 or BPAY means a Service which allows you to make BPAY payments electronically. We are a member of the BPAY Scheme. We will tell you if we cease to be a member of the BPAY Scheme.

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

Business Day means a weekday including local public holidays but excluding holidays observed on a national basis.

Card means the credit card issued by us in accordance with the Bankwest Credit Card Conditions of Use and includes where applicable, a Virtual Card.

Card Conditions of Use means the specific Conditions of Use we provide to you together with these Credit Card Account Access Conditions of Use and which we tell you form part of the Card contract.

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

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

Confirmation of Payee means the service that may allow you to confirm the account name of the BSB and account number you want to make a payment to.

Credit Card Scheme Rules means, as relevant, the credit card rules of Mastercard International Incorporated.

Easy Alerts means the legacy Bankwest notification service allowing customisation of push notifications preferences.

EFT System means the 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 an account with us 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.

Eligible Recipient Account means an account:

- which is maintained by an ADI which is a subscriber to the ePayments Code;
- that belongs to an identifiable individual in whose name a facility has been established by the subscriber.

ePayments Code means the ePayments Code issued by ASIC.

Financial abuse is a serious form of domestic and family violence that may occur through a pattern of control, and results in exploitation or sabotage of money and finances which affects an individual's capacity to acquire, use and maintain economic well-being and which threatens their financial security and self-sufficiency.

Merchant means a supplier of goods or services.

Mobile Device means a mobile telephone or other small screen device which can be used to access the Internet.

Mistaken Internet Payment means a payment initiated using the Pay Anybody service described in clause 4.2 from your account where funds are paid into an Eligible Recipient Account of an unintended recipient because a User enters or selects a BSB number and/or identifier that does not belong to the named and/or intended recipient as a result of:

- the User's error, or
- the User being advised of the wrong BSB number and/or identifier.

This does not include payments made using BPAY.

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.

NameCheck means the technology we may use when you make a payment using a BSB and account number to:

- give you a view on the likelihood that the account name you enter matches the account; and
- prompt you to take further steps to ensure you are paying the intended recipient.

This does not confirm that the name actually matches the account.

NameCheck prompts are based on our available payment information and used to enhance the Confirmation of Payee service.

NFC means near field communication.

Payment Device means an NFC enabled payment accessory (other than a Mobile device or Card) including without limitation a ring, key fob or other device which is NFC enabled and which is provided to you and owned by us to make payments from your Card account.

PAN means a personal access number allocated to a User by us to identify the User for the purposes of accessing Phone Banking and Bankwest Online Banking.

Password (also known as secure code) means the Access Method required by users, along with a PAN, to access Phone Banking or Bankwest Online Banking. For Phone 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 or Payment Device, as changed by you or us from time to time.

Receiving ADI means an ADI which is a subscriber to the ePayments Code and whose customer has received a payment which you have reported as being a Mistaken Internet Payment.

Recurring Payment means a payment arrangement by which you have given your Card Details to a merchant or service provider to charge your account at intervals agreed by you (including on a one-off or ad hoc basis).

Secret Code means individually and collectively a User's PIN, Token Code, Password, Token PIN, answers to your Secret Questions, SMS Code, any code we give you to authenticate a user or transaction and code to unlock a mobile device, change settings on 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.

Service means Phone Banking, or Bankwest Online Banking, including the BPAY Scheme or Pay AnyBody service.

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.

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 Additional Cardholder.

Virtual Card means a type of Card that from 19 March 2025:

- may be provided to you to access the Card Account on the terms set out in your Card Contract via a request made by you through the Bankwest App;
- that exists solely in virtual (digital) form (i.e. a Virtual Card is not available in physical form);
- uses Mastercard payment infrastructure;
- contains Card Details not replicated on any other Mastercard issued in connection with the Card Account; and
- may be used either on a single-use basis, or a multi-use (see section 2.2 in Part 2 of these Account Access Conditions of Use).

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 holder of the Card account. 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, the Secret Questions Security, and where applicable for the purpose of consistency with the ePayments Code, where relevant, “you” also includes any User.

1.2 ePayments Code

We will comply with the requirements of the ePayments Code where those requirements apply to your dealings with us.

1.3 Changes

Acting reasonably, we can change these Credit Card 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, your Card account or Electronic Equipment.

Subject to any applicable law or code of conduct:

– we will notify you of other changes no later than the day that the change takes effect; or

– where an immediate change is necessary to manage a material and immediate risk, or to restore or maintain the security of the EFT System or an account, we may make a change necessary for that purpose without giving you advance notice.

We may notify you of changes by

(a) the electronic means described in clause 1.4;

(b) a notice on or with your Card account statement;

(c) publishing a press advertisement; or

(d) notices on EFT terminals.

Changes in your personal details

You must inform us immediately of any change in your name or address including changes to your nominated mobile phone number or other electronic address. You can do this by messaging us in the Bankwest App or by telephoning our Contact Centre.

1.4 Electronic Communications

Where you have given us an email address, mobile phone number or other electronic address for contacting you, you agree that we may satisfy any requirement under these Credit Card Account Access Conditions of Use or under any law or applicable code of conduct to provide Users with information by any of the following means:

(a) electronic communication to your nominated electronic address;

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

- SMS message to a mobile phone number you have given us for contacting you;
- by electronic communication to any other electronic address you have given us for contacting you, or
- push notification from the Bankwest App that the information is available for retrieval by you;

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

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

You acknowledge we have advised you that:

- Your agreement for us to communicate with you by electronic communication may be cancelled by you at any time by notice to us. You may also change any email address, mobile phone or other electronic address via the Bankwest App or by calling us on 13 17 19.
- While you have agreed that we can communicate with you by electronic communication, paper communications may no longer be given to you and you should regularly check your electronic communications for notices and statements from us.

Should we provide you with information by an electronic method outlined in this clause, 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).

Marketing and commercial messages

This clause relates to the marketing and commercial electronic messages we may send you. By this clause you consent to receiving those messages, but you have the option to withdraw that consent and tell us not to send them.

If you provide us with your contact details (such as your email and telephone number) you agree that we may use them to communicate with you (unless you tell us not to), including:

- to send you commercial electronic messages;
- for direct marketing purposes; and
- to make phone calls to you for an indefinite period, in accordance with Schedule 2 of the Do Not Call Register Act 2006 (Cth), unless you tell us not to.

By registering for online services (such as Bankwest Online Banking) or accessing Bankwest applications (such as the Bankwest app), you also agree that (unless you tell us not to) we may send you commercial electronic messages and/or direct marketing through these online services and applications (including push notifications, in-app messages and notifications, or messages to your Bankwest Online Banking inbox).

You agree that each time you use an automated digital assistant that is available in our online services or applications, we may send you commercial electronic messages or direct marketing through that assistant's response to you.

Sometimes we use third party service providers such as marketing companies or mail houses to send messages on our behalf for direct marketing purposes. You agree that (unless you tell us not to) we may share your personal information with marketing companies or mail houses so they can send you direct marketing messages and commercial electronic messages.

Changing your preferences

We will provide you with options you may use to opt out of receiving commercial electronic messages we send you and to choose the way we send them to you. While in some cases one of the options may be an unsubscribe facility, you agree we are not required to include an unsubscribe facility in commercial electronic messages we send you.

Opting out of commercial electronic messages may impact our ability to provide you with information about all the benefits that are available as our customer. There are, however, messages that we must be able to send you and which you will not be able to opt out of receiving.

1.5 Cancellation of electronic access

We may, in our discretion, and without liability to you:

- withdraw or deny access to a Service;
- cancel or suspend any Card or Payment Device, refuse to process or complete (eg block or decline), or hold or delay the processing of, a transaction or dealing of a User; or
- cancel electronic access to your Card account, at any time without prior notice, in certain circumstances including (but not limited to):
    - if we reasonably consider it necessary to:
        - comply with our financial crimes policies, any laws in Australia or laws overseas, or card scheme rules; or
        - manage any risk;
    - if we reasonably consider that your Card account or a User's access method or the transaction, dealing or type of transaction or dealing may be being used unlawfully including fraudulently or as part of a possible scam or in any way that might otherwise cause you or us to lose money;
    - if a User seeks to make a payment to an account or type of account which we reasonably believe may be being used unlawfully including fraudulently or as part of a possible scam or in any way that might otherwise cause you or us to lose money;
    - if a User seeks to make a payment to an account which we reasonably believe may be owned or by controlled by a crypto-currency or digital asset exchange;
    - if a User's transaction instructions are not clear;
    - if we reasonably consider there has been non-compliance with these Credit Card Account Access Conditions of Use;
    - if you do not provide us with any document or information we reasonably request from you;
    - if we reasonably consider there has been unsatisfactory account operation, including conduct that, in our opinion:
        - is defamatory, harassing or threatening to any person;
        - promotes or encourages physical or mental harm of any person;
        - promotes violence against any person; or
        - threatens or promotes terrorism;
    - if we reasonably consider that a User may be a person, acting for or conducting business with a person:

- with whom we are not permitted to deal with by law or a regulatory authority; or
- in breach of laws relating to money laundering and terrorism financing.
- if we reasonably suspect a User is residing in a sanctioned jurisdiction or travelling to a sanctioned jurisdiction (while the User is in that jurisdiction). To find out the current list of sanctioned jurisdictions please visit commbank.com.au/sanctioned countries (this list may change from time to time without notice to you)
- if we reasonably consider that you have not complied with the requirements for your Security Setting; or
- if we reasonably consider a security issue has arisen which requires further investigation.
- if we suspect on reasonable grounds that your account is being used in a way that results in or may cause financial abuse.

We will not be responsible for any cost, expense or other inconvenience you incur when we exercise our discretion to withdraw or deny access to a Service, cancel or suspend a Card, refuse to process or complete (eg block or decline), or hold or delay the processing of, a transaction or dealing of a User, or cancel electronic access to your Card account.

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 your Card account is cancelled by you or us, you must, if relevant, halt the use of any Payment Device, Card or Security Token, ensure that all cards are returned to us cut in half diagonally or otherwise satisfy us that they have been destroyed, and return the Security Token to us undamaged.

Notwithstanding the above, we may cancel your use of a Service, Card or Payment Device at any time on providing reasonable notice to you. The Bank has an obligation under the Banking Code of Practice to act fairly and reasonably towards you in a consistent and ethical manner.

You may end your use of a Service or cancel a User's electronic access to your Card account at any time by calling our Contact Centre, or by messaging us in the Bankwest App.

1.6 Additional Cardholders

You agree that you are responsible to ensure that Additional Cardholders comply with these Credit Card Account Access Conditions of Use and to ensure that each Additional Cardholder protects their Access Method in the same way as these Credit Card Account Access Conditions of Use require you to protect your Access Method.

1.7 Access to a nominated cheque or savings account

Account access to a nominated account by a User is not governed by these Conditions of Use but by the Bankwest 'Account Access Conditions of Use'. Users should refer to those 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 your 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.

1.8 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 Credit Card 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 calling us on **13 17 19**.

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 Credit Card 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 Codes 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 (and our approval will not be unreasonably withheld). 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. Call us on **13 17 19**.

Part 2 – Card Conditions of Use

2.1 About this Part

This Part (together with Parts 1, 6, 7, 9 and 10) applies to all transactions involving the use of the Card itself or the Card Details or a Mobile Wallet to access your Card account.

2.2 Access to your 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 appropriate Card symbol. In Australia you will usually need to enter a PIN. If a Merchant accepts payment with your Card by mail order, telephone or online, users 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) ATM users may use their Mastercard and PIN to obtain cash advances in Australia and overseas at ATMs displaying the appropriate symbol. You cannot use a Virtual Card to obtain a cash advance at an ATM or elsewhere.

(c) Single-use Virtual Cards will no longer be usable after a single transaction or after 24 hours of issuance (whichever occurs first). This is the case regardless of the card expiry date that appears on the Card.

(d) For multi-use Virtual Cards, the following applies:

- you may set an optional spend limit;
- you must select a card end date; and
- if you set an optional spend limit for your Virtual Card, subject to the available balance on your Card Account, you may make multiple transactions using the card until either (i) the spend limit is reached or (ii) the card end date is reached (whichever occurs first). The card will no longer be usable after the occurrence of one of these events. This is the case regardless of the card expiry date that appears on the Card.

2.3 How much cash can you get?

(a) Subject to paragraph 2.3 (b), the minimum amount a User can obtain each day from CBA 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 and our agents may set their own limits.

Cash advances may not be obtained using EFTPOS terminals.

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.

(b) 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 Card account has operated and your payment history.

2.4 Paying bills using your 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 your 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 the Card account at selected agents and select CBA ATMs. There are limits on the amount of cash you can deposit at our agents and ATMs. If a cheque is deposited the proceeds of the cheque will not be available until the cheque is cleared. If funds are deposited into your Card account we may hold the funds until we have complied with requirements under any relevant laws in Australia or any other country (for example anti-money laundering and counter-terrorism financing laws).

All deposits made at CBA ATMs are checked by us. If the amount appearing on the transaction record differs from the amount received by us, we will credit your Card account with the amount actually received and notify you as soon as possible.

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 accept responsibility for the security of deposits received at CBA ATMs subject to checking of the amount deposited. The amount checked by us is evidence of the amount actually received.

A Virtual Card cannot be used to deposit funds.

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 your Card account on the day they are made. Processing may take a number of days. We will process transactions to your Card account as soon as practicable.

Users should observe the guidelines set out in Clause 6.2 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 the Card account may need to be authorised by us. We may at our discretion and acting reasonably decline a transaction (or any category of transaction) for any reason, including but not limited 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 credit limit would be exceeded, 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.

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 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 and the ePayments Code, 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 Merchant's premises does not mean 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. However, please refer to Clause 9.1 where a 'chargeback' right may be available under the Credit Card scheme rules.

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 your 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 from 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, 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, reported lost or stolen or its balance written off.

A Card of an Additional Cardholder cannot be deleted or cancelled in a Mobile Wallet, however, you may suspend or cancel an Additional Cardholder's Card by messaging us in the Bankwest App or calling us 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 your 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, other than to the extent that the loss was directly caused by our act or omission. 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 suspect on reasonable grounds that your account is being used in a way that results in or may cause financial abuse.

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

2.10 When we may block or decline a transaction

You may only use your Card or Payment Device for lawful purposes.

In addition to our rights under clause 1.5 (“Cancellation of electronic access”), we may block or decline purchases from certain websites or merchants if we have reason to believe that the products or services being offered:

- are illegal in Australia or elsewhere;
- contain offensive material;
- pose a risk to the function or integrity of information systems or data;
- may be used unlawfully including fraudulently or as part of a possible scam or in any way that might otherwise cause you or us to lose money or to otherwise manage risk;
- are from an account which we reasonably believe may be owned or controlled by a crypto-currency or digital asset exchange.

Part 3 – Phone Banking and Bankwest Online Banking Conditions Of Use

3.1 About this Part

This Part (together with Parts 1, 6, 7 and 9) applies to use of Phone Banking and Bankwest Online Banking in connection with your Card account.

3.2 What is Phone Banking?

Phone Banking is a Service which enables a User to make enquiries and effect transactions on your 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 Phone Banking?

Users can:

- obtain the balance of your Card account;
- transfer funds between accounts;
- enquire about transactions on your Card account;
- make payments to your Card account;
- make bill payments electronically through BPAY;
- postdate funds transfer and bill payments up to 90 days in advance;
- order a statement of interest for taxation purposes; and
- change a Password.

3.4 How to use Phone Banking

To use Phone 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 that is accessible via a computer or mobile device with internet access, and a mobile device using the Bankwest App, which enables a User to make enquiries and effect transactions over the Internet on your Card account using a PAN and Password. Bankwest Online Banking must only be accessed via an Approved Browser.

The Bankwest App is available for compatible iPhone, iPad and Android™ devices offering a fast, simple and convenient mobile banking experience. With the Bankwest App you can check account balances, view recent transaction history, pay bills via BPAY, make transfers to linked and third party accounts from your smart phone. Additionally, you can locate your nearest Commonwealth Bank ATM.

In order to access the full range of Bankwest App features, security and other updates, you should ensure that you use the latest version of the Bankwest App. You may need to upgrade the operating system on your device to ensure it is compatible with the latest Bankwest App version.

If you access our website from a mobile device or use the Bankwest App, you may not be able to access the full range of services which are ordinarily available from our website.

3.6 What can be done using Bankwest Online Banking?

Features available in Bankwest Online Banking include:

- obtain the balance of your Card account;
- transfer funds between accounts;
- enquire about transactions on your Card account;
- check past statements on your Card account;
- order a printed statement on your Card account;
- make payments to your Card account;
- make bill payments electronically through BPAY;
- postdate funds transfer and bill payments;
- order a statement of interest for taxation purposes;
- change a Password;
- lodge various service and application forms with us;
- close a Card account;

– make a Pay AnyBody transfer (see Part 4).
– perform a range of administrative functions; and
– manage communication preferences (including push notifications which we may send from time to time).

In addition to the Bankwest App, we provide a version of Bankwest Online Banking that has been customised for Mobile Devices using internet browser software. 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 internet browsing software, or the Bankwest App, and other functions may operate with a reduced or different level of functionality.

If you have the Bankwest App installed on an iPhone or iPad, you can turn on:

– Touch ID for the Bankwest App: where you can access the Bankwest App using a fingerprint identity sensor (except for iPhone X onwards); or
– Face ID for the Bankwest App: where you can access the Bankwest App using facial recognition ability for iPhone X onwards.

If you have the Bankwest App installed on an Android mobile device, you can choose the option of using fingerprint recognition to access the Bankwest App.

If you turn on Touch ID, Face ID or use Android fingerprint recognition on the Bankwest App, you consent to Bankwest collecting the biometric information you provide for the purposes of identifying you and otherwise for use in accordance with the Bankwest Privacy Statement.

For certain transactions on the Bankwest App, you may be prompted to enter your Bankwest App PIN Login as an additional security measure.

You must only store your own biometric identifiers (including your fingerprints or your facial mapping) on your smartphone device. You must not use Touch ID, Face ID or use Android fingerprint recognition on the Bankwest App if you have someone else's biometric identifiers, including their fingerprints or facial mapping stored on your device.

If you do allow someone else's fingerprints or facial mapping to be stored on your device (despite this being against these Conditions of Use):

– They will be able to access your accounts and will be considered authorised to do so; and
– You will be responsible for their transactions.

Touch ID, Face ID and Android fingerprint recognition can only be turned on for the Bankwest App if it is available on your mobile device model and has been enabled by you on your device. Touch ID, Face ID and Android fingerprint recognition are technologies provided by vendors external to Bankwest and accordingly we are not responsible:

– For any malfunction in such technologies; or
– If Apple or Android make any changes to their technology that impacts the way you access the Bankwest App, e.g. For iPhone X users, effective from 3 November 2017, the fingerprint sensor will no longer be available and is replaced with facial recognition ability.

If you choose to use Touch ID, Face ID and/or Android fingerprint recognition to access the Bankwest App, you will still need your internet banking login details and you must protect these in the manner outlined in these Conditions of Use.

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 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 using internet browser software 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 and mobile device is free of viruses;
- ensuring their computer and mobile device 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 6 of these Credit Card Account Access Conditions of Use and the ePayments Code.

3.9 Access and restriction of access to Services

Access to Phone 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.

You may not be able to access Bankwest Online Banking from all computers or Mobile Devices due to hardware or software restrictions, connection limitations, the capacity of your internet service provider, availability of a connection via your telecommunications provider/carrier or for other reasons outside our control.

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 7.4, 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, other than to the extent that the loss or damage is directly caused by out act or omission.

You are responsible for any fees or charges imposed by a telecommunications provider/carrier for accessing Phone 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 Phone Banking or Bankwest Online Banking instruction without notifying you. Instructions will not be processed:

- when your Card contract prohibits the payment(s);
- when the credit limit of the Card account would be exceeded; or
- when a BPAY payment will cause you to exceed your daily BPAY payment limit.

You should ensure that any transaction instruction you give would not cause your credit limit to be exceeded. Except for BPAY and Pay

AnyBody transactions, transactions made prior to 6:00pm 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.

3.9A Refusal of Service

Acceptable Use Policy

You may not use Bankwest Online Banking to engage in conduct that, in our opinion:

- is unlawful;
- interferes with any other person's access to Bankwest Online Banking;
- is used for a vehicle for, or may cause or result in financial abuse;
- is offensive, defamatory, harassing or threatening to any person;
- promotes violence against any person; or
- threatens or promotes terrorism.

In the event that you fail to comply with our Acceptable Use Policy as detailed above, we may, without notice and immediately or at any time:

(a) refuse to process or complete any transaction or dealing of yours; and/or

(b) suspend or discontinue your access to Bankwest Online Banking.

If we receive a complaint or request from or on behalf of a recipient of a transaction or dealing of yours using Bankwest Online Banking, we may investigate and consider in light of Bankwest's Acceptable Use Policy. You acknowledge and agree that we may respond to a complaint or a request by sharing the outcome of such investigation, including any related action taken against you.

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 credit limit 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

Acting reasonably, at our discretion we may impose and/or vary minimum and/or maximum limits on the amounts which you may transfer from your Card account using our Services. Current information on these limits can be accessed by logging in to Bankwest Online Banking, messaging us in the Bankwest App or calling us on **13 17 19**.

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.

3.13 Authorised users

Each Additional 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 the Credit Card Account Access Conditions of Use, Clause 3.14 prevails to the extent of that inconsistency.

(b) When you tell us to make a BPAY payment, you must give us the information specified in paragraph (f) below. We will then debit your 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) Phone 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 Phone 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.

You may request this limit to be changed:

i. online after registering for SMS Code Security or Secret Questions Security; or.

ii. by contacting us.

Approval of limit changes is subject to our sole discretion.

Current information on limits can be accessed by logging in to Bankwest Online Banking, messaging us in the Bankwest App or by calling us on **13 17 19**.

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 credit limit of the Card account or the daily Bpay payment limit to be exceeded.

(h) If there is any inconsistency between this Clause 3.14 and any other part of these Credit Card Account Access Conditions of Use, this clause prevails to the extent of that inconsistency.

(i) A Bpay payment from the Card account is treated as a purchase transaction.

(j) Except for postdated payments (Clause 3.14 (o)) we will not accept an order to stop a Bpay payment once we have been instructed to make the Bpay payment.

(k) 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 4:00pm WST on a business day; or

ii. on the next business day, if we receive the instruction after 4:00pm WST on a business day, or on a non-business day.

(l) 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.

(m) 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.

(n) If we are advised that a BPAY payment cannot be processed by a biller, we will advise you, credit your 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.

(o) 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 your credit limit, your daily BPAY payment limit or any other limit we impose in accordance with Clause 3.11 is exceeded, it will be necessary to resubmit 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.

(p) We may charge a fee to correct errors on your Card account due to incorrect BPAY instructions.

(q) 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.

(r) You should check your 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).

(s) Your liability for unauthorised and fraudulent BPAY payments will be determined in accordance with Part 7 of these Credit Card Account Access Conditions of Use.

(t) Disputes in relation to unauthorised, fraudulent or wrong BPAY payments will be handled in accordance with Part 9 of these Credit Card Account Access Conditions of Use, however, no chargeback rights are available in respect of a BPAY payment from your Card account.

(u) **If we make the wrong payment**

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 your Card account was debited with the payment, we will credit that payment amount to your account.

(v) **Biller consent**

If you tell us that a BPAY payment made from your 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.

(w) **Consequential damage and indemnity**

Subject to Part 7 of these Credit Card Account Access Conditions of Use and the ePayments Code:

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 the fraud, negligence, mistake or willful misconduct of us, our employees or agents, or in relation to any breach of a condition or warranty implied by law under consumer protection legislation 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.

– However, this indemnity does not apply to the extent that the loss or damage was caused directly by the fraud, negligence, mistake or willful misconduct of us, our employees or agents.

Part 4 – Pay AnyBody Conditions of Use

4.1 About this Part

This Part (together with Parts 1, 6, 7 and 9) applies to all transactions involving the use of the Pay AnyBody Service (Pay AnyBody). Pay AnyBody is an extension of Bankwest Online Banking (see Part 3). If there is any inconsistency between this Part and Part 3, this Part prevails to the extent of that inconsistency.

4.2 What is Pay AnyBody?

Pay AnyBody is a Service available via Bankwest Online Banking which allows a User to transfer funds from an account with us 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, by using the BSB number, account number and account name for the other person's account.

4.3 Daily Pay AnyBody transfer limit

The initial maximum aggregate amount of Pay AnyBody payments (including Faster Payments) that you may instruct us to make on any business day is $1,500. You may request this limit to be changed:

a. online after registering for SMS Code Security or Secret Questions Security; or

b. by contacting us.

Approval of limit changes is subject to our sole discretion.

Current information on these limits can be accessed in Bankwest Online Banking, by calling our Contact Centre on 13 17 19 or messaging us in the Bankwest App.

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) To make a Pay AnyBody transfer you must enter the BSB number, account number and account name in respect of the account to which the funds are to be transferred, together with a description of the transaction. If you are making a payment using a BSB and account number, it is your responsibility to ensure the BSB and account number are correct. You may use Confirmation of Payee (enhanced with our NameCheck technology) to confirm the account name of the BSB and account number you want to make a payment to or to give you a view on the likelihood that the account name you enter matches the account and prompt you to take further steps to ensure you are paying the intended recipient. If the Confirmation of Payee result indicates that the details do not look right, we strongly recommend you check the information entered and re-confirm the details with the intended recipient. We may limit or suspend your use of Confirmation of Payee if we believe it is reasonably necessary to protect you or us from possible fraudulent activity, scams or other activities that might cause you or us to lose money.

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 credit limit of the card account or your daily Pay AnyBody transfer limit to be exceeded.

(b) 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 transfer if the requirements of Clause 3.10 are met. If the date stipulated is not a business day, we will make the 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 is payable for any such cancellation.

4.7 Processing Pay AnyBody transfers

(a) Generally, a Pay AnyBody transfer will be treated as received:

- on the date we are told to make that Pay AnyBody transfer, if we receive the instruction before 3:00pm WST on a business day; or
- on the next business day, if we receive the instructions after 3:00pm WST on a business day, or on a non-business day.

Delays may arise because we need to verify that the transaction is an authorised transaction or due to the conduct of the recipient financial institution for which we will not be responsible.

(b) If we are advised that a Pay AnyBody transfer cannot be processed by another financial institution, we will advise you, credit your 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.

4.8 If we make the wrong payment

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

4.9 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.

4.10 Mistakes as to the account to which a Pay AnyBody payment is made

(a) Under the ePayments Code, there are certain processes regarding Mistaken Internet Payments that we and many other ADIs have adopted. They do not apply to transactions where the Pay Anybody service used is a service designed primarily for use by a business and established primarily for business purposes. These processes (which we agree to follow) are set out below. We will not otherwise have liability to you for Mistaken Internet Payments under this clause.

(b) Overview

i. You must report a Mistaken Internet Payment as soon as possible. For how to report a Mistaken Internet Payment, see clause 4.10(c).

ii. We will acknowledge each report you make and investigate whether a Mistaken Internet Payment has been made.

iii. If the relevant payment has been made to a Bankwest or CBA-branded Eligible Recipient Account, but we don't agree that it was a Mistaken Internet Payment, we may (but are not obliged to) ask the consent of the recipient to return the funds to you. If consent is given, we will return the funds to you as soon as practicable.

iv. If a Mistaken Internet Payment has been made to a Bankwest or CBA-branded Eligible Recipient Account held with us, we will return to you any funds we retrieve from the recipient. The process setting out how we retrieve Mistaken Internet Payments from the unintended recipient is set out in sub clause 4.10(d).

v. If a Mistaken Internet Payment has been made to an Eligible Recipient Account held with another ADI, we will return to you any funds the Receiving ADI provides to us as soon as practicable. The process setting out how we retrieve Mistaken Internet Payments from a Recipient ADI is set out below in sub-clause 4.10(e).

vi. Generally, we will return funds to you by crediting the account from which the Mistaken Internet Payment was made. If you no longer have an account with us, or if it is not practicable to credit returned funds to that account, we will return funds to you by some other means.

vii. You may not retrieve the full value of your payment if:

- we or the Receiving ADI do not think that a Mistaken Internet Payment has occurred (including because the payment you made was not to an Eligible Recipient Account); or
- we or the Receiving ADI do not retrieve the full value of a Mistaken Internet Payment from the unintended recipient.

viii. In any case, we will inform you of the outcome of your report of a Mistaken Internet Payment within 30 business days of you making it.

ix. If you are not satisfied with how your report has been handled (by us or the Receiving ADI) or the outcome of your report, you can lodge a complaint with us. See Part 9 regarding how to lodge a complaint and how we will handle that complaint.

(c) You may report a Mistaken Internet Payment by:

- telephoning our Contact Centre on **13 17 19**;
- if you are overseas, telephoning us on **+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).
- messaging us in the Bankwest App; or
- writing to us at GPO Box E237, Perth WA 6841.

We will advise you of the steps you must take so we can investigate the matter. You must give us full details of the transaction you are querying.

In order for us to investigate the payment, you must contact us promptly by messaging us in the Bankwest App or calling our Contact Centre on **13 17 19**. We will contact you if we require further information, and you must supply this information within 10 business days.

(d) This sub clause 4.10(d) applies if we have determined that a Mistaken Internet Payment has been made to a Bankwest or CBA-branded Eligible Recipient Account.

i. Despite paragraphs 4.10(d) (ii) and (iii) below, if the unintended recipient is receiving Services Australia income support payments or Department of Veterans' Affairs payments, we will recover the funds from the unintended recipient in accordance with the *Code of Operation:*

Recovery of debts from customer nominated bank accounts in receipt of Services Australia income support payments or Department of Veterans' Affairs payments.

ii. If the account into which the Mistaken Internet Payment was made does not have sufficient credit funds to return the full value of the payment, we (or CBA, as relevant) may debit the unintended recipient account for a partial or full amount of the Mistaken Internet Payment in accordance with the process and relevant timeframes described in 4.10(d)(iii) below. If we (or CBA, as relevant) choose to retrieve the full value of the funds from the unintended recipient account, we (or CBA, as relevant) will use reasonable endeavours to do so.

iii. If the account into which the Mistaken Internet Payment was made has sufficient credit funds to cover the full value of the payment, the following applies:

- If you have reported the Mistaken Internet Payment within 10 business days after the payment is made, we will return the funds to you. We will do this within 5 business days of determining that the payment is a Mistaken Internet Payment if practicable, although we may reasonably delay the payment up to a maximum of 10 business days.
- If you have reported the Mistaken Internet Payment between 10 business days and 7 months after the payment is made, we will give the unintended recipient 10 business days to establish that they are entitled to the funds. If they do not establish this, we will return the funds to you within 2 business days after the expiry of that period.
- If you have reported the Mistaken Internet Payment more than 7 months after the payment is made and the recipient's account has sufficient credit funds, we will ask the unintended recipient if they agree to the return of the funds to you. If they agree, we will return the funds to you as soon as practicable.

(e) If we have determined that a Mistaken Internet Payment has been made to an Eligible Recipient Account that is not a Bankwest or CBA-branded account, we will follow the ePayments Code process to attempt to retrieve your funds. This process is set out below.

i. We will send the Receiving ADI a request for the return of the funds. The Receiving ADI is required to acknowledge this

request within 5 business days and let us know whether there are sufficient funds in the unintended recipient's account to cover the payment.

ii. Despite paragraphs 4.10(e)(iii)-(v) below, if the unintended recipient is receiving Services Australia income support payments or Department of Veterans' Affairs payments, the Receiving ADI must recover the funds from the unintended recipient in accordance with the *Code of Operation: Recovery of debts from customer nominated bank accounts in receipt of Services Australia income support payments or Department of Veterans' Affairs payments*.

iii. If the account into which the Mistaken Internet Payment was made does not have sufficient credit funds to return the full value of the payment, and the Receiving ADI agrees that a Mistaken Internet Payment has been made, the Receiving ADI may debit the unintended recipient account for a partial or full amount of the Mistaken Internet Payment in accordance with the process and relevant timeframes described in 4.10(e)(iv) below.
If the Receiving ADI chooses to retrieve the full value of the funds from the unintended recipient account, they must use reasonable endeavours to retrieve the funds from the recipient for return to you.

iv. If the account into which the Mistaken Internet Payment was made has sufficient credit funds to cover the payment, the following applies:

- If you have reported the Mistaken Internet Payment within 10 business days after the payment is made and the Receiving ADI agrees that a Mistaken Internet Payment has occurred, the Receiving ADI is required to return the funds to us within 5 business days of receiving our request if practicable, although the Receiving ADI may reasonably delay the payment up to a maximum of 10 business days.
- If you have reported the Mistaken Internet Payment between 10 business days and 7 months after the payment is made, the Receiving ADI has 10 business days to investigate whether the payment is a Mistaken Internet Payment. If the Receiving ADI agrees that a Mistaken Internet Payment has occurred, it will give the unintended recipient 10 business days to establish that they are entitled to the funds. If they do not establish this, the Receiving ADI must return the funds to us within 2 business days after the expiry of that period.

- If you have reported the Mistaken Internet Payment more than 7 months after the payment is made, and the Receiving ADI agrees that a Mistaken Internet Payment has occurred, the Receiving ADI must ask the unintended recipient if they agree to the return of the funds.

v. If the Receiving ADI doesn't agree that a Mistaken Internet Payment has occurred, it may (but is not obliged to) ask the consent of the recipient to return the funds.

vi. If the recipient agrees to the return of the funds, the Receiving ADI must return the funds to us.

Part 5 – Recurring Payments

5.1 About this Part

This section provides you with information about Recurring Payments.

5.2 Maintain a record of any Recurring Payments

Cardholders are encouraged to maintain a record of any Recurring Payments they elect to enter into with a Merchant. You can ask us for a list of any Recurring Payments for up to the previous 13 months.

5.3 Changing Recurring Payments

To either change or cancel a Recurring Payment, you should contact the Merchant at least 15 days prior to the next scheduled payment and if possible you should retain a copy of the change/cancellation request made to the Merchant.

Until you attempt to cancel the Recurring Payment we must accept any instructions received from the Merchant. If a merchant is registered for the Mastercard Automatic Billing Updater service, your Recurring Payment to the merchant will continue after your Card has been changed to a new product, replaced due to damage, or after an old Card has expired and a new Card issued in its place. This is because the Mastercard Automatic Billing Updater service automatically informs those merchants of your replacement Card details, so that your Recurring Payment is not interrupted.

Please note that if we have issued you with a new Card to replace a Card that was lost, stolen, or subject to possible fraud, the Card details of that new Card will not be subject to the Mastercard Automatic Billing Updater service.

Change of Card Details

Should your Card Details change, you must request the Merchant change the details of the existing Recurring Payment to ensure it continues. If you fail to make this request your Recurring Payment either may not be honoured by us, or the Merchant may stop providing the goods and/or services.

However, if we issue new Card details to you due to the re-issue of an expired Card, the replacement of a Card due to damage, or a changed Card product, your Recurring Payment will continue uninterrupted to merchants who are registered for the Mastercard Automatic Billing Updater service. Given that not all merchants are registered for the Mastercard Automatic Billing Updater service, you remain responsible for giving your new Card details to the merchant you wish to pay via a Recurring Payment. Please note that if we have issued you with a new Card to replace a Card that was lost, stolen, or subject to possible fraud, the Card details of that new Card will not be subject to the Mastercard Automatic Billing Updater service. This means that you must request the merchant to change the details of the existing Recurring Payment to ensure it continues.

Should you elect to close your Card account or we close your Card account you should contact the Merchant to revise your Recurring Payment as the Merchant may stop providing the goods and/or services.

Part 6 – Security of Access Methods

6.1 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.

6.2 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 7 of these Credit Card Account Access Conditions of Use and the ePayments Code.

To protect the Card:

- sign the Card as soon as it is received;
- carry the Card whenever possible;
- always keep the Card in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- never lend the Card to anybody or permit any other person to use the Card or Card Details; and
- when the transaction is complete remember to take the Card and the transaction receipt.

To protect the Card Details:

- do 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:

- 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 furniture;
- do not keep a record of the Secret Code with any document containing the reference numbers for the Card account such as statements; 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:

- 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
- do not access Phone 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:

- carry the Security Token whenever possible;
- always keep the Security Token in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- do not record account numbers, your PAN, or Secret Code details on the Security Token;
- do not drop the Security Token or expose it to high heat, water or attempt to dissemble it;
- do 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;
- do not lend the Security Token to anyone, or permit anyone to use the Security Token.

To protect the security of a Mobile Wallet:

- the user should ensure that any secret code we give a user to establish a Mobile Wallet on a mobile device should not be disclosed to anyone else;
- 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;
- 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;
- 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;
- a User must not act with extreme carelessness in relation to the security of the secret code;
- 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;

- a User must install and regularly update anti-virus software on the mobile device;
- 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
- a User must remove any Card from the User's mobile device before disposing of the mobile device.

To protect the Payment Device:

- keep the Payment Device in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- do not expose the Payment Device to high heat, or attempt to dissemble it or keep it near electromagnetic fields;
- do not keep the Payment Device with any document containing the reference numbers for nominated accounts or with other account information such as statements or cheque books; and
- do not lend the Payment Device to anyone, or permit anyone to use the Payment 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 User's mobile device is disconnected without the knowledge or permission of the User; or
- 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.

Part 7 – Loss, Theft or Unauthorised Use of Your Access Method

7.1 What users have to do

If:

- any Card;
- Payment Device;
- 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 Additional Cardholder must immediately tell us or, in the case of a Card or Payment Device, 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 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.

7.2 What is your liability for unauthorised EFT Transactions?

You are liable for all EFT Transactions carried out in respect of your Card account with the knowledge and consent of a User, including where we use our NameCheck technology to give you a view on the likelihood that the account name you enter matches the account and to prompt you to take further steps to ensure you are paying the intended recipient, except where a Mobile Wallet is used. Part 7A deals with liability for transactions made using a Mobile Wallet.

7.2.1 When you are not liable

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

- before the User has received their Card, Payment Device, 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 where the secret code has become 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.

7.2.2 When you are liable

You will be liable for losses in respect of a Card account caused by an unauthorised EFT Transaction where we prove on the balance of probabilities that the User has contributed to losses 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**:

    i. voluntarily disclosing the Token PIN, **or**

    ii. 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 Payment Device or Security Token, or breach of the security of the Secret Code; or by unreasonably delaying notifying us of the unauthorised use, theft or loss of the Card, Payment Device 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, Payment Device 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;

(e) that portion of the loss which exceeds the credit limit of the Card account; or

(f) losses directly incurred as a result of our act or omission.

7.2.3 When your liability is limited

Where a Secret Code was required to perform the unauthorised EFT Transaction and Clause 7.2.2 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 you notify us 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 credit 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.

7.2.4 Notwithstanding any of the provisions contained in this clause, your liability will not exceed your liability under the ePayments Code.

7.3 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.

7.4 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 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 your Card account and the refund of any charges or fees imposed on you as a result.

Please advise us if an EFT Terminal has a service fault or difficulty. Users can do this by telephoning us or by messaging us in the Bankwest App.

Part 7A – Liability For Mobile Wallet Transactions

7A.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.

7A.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 6.2.

7A.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 where the secret code has become known to someone else;

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

  i. us;

  ii. any organisation involved in the provision of the EFT system; or

  iii. 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 transaction being incorrectly debited more than once to the same account.

Part 8 – Payment Device Conditions of Use

8.1 About these conditions

If your Card account is of a type that we have determined may be linked to a Payment Device, Part 8 (together with Parts 1, 6, 7, and 9) of these Conditions of Use applies to all transactions involving the use of:

- tapping the Payment Device and entering a user's PIN to make payments at merchant terminals; and
- the Payment Device to make contactless payments at merchant terminals from your Card account.

There is a limit of one Payment Device per User for each Card account and a Payment Device cannot be used to access more than one Card account.

8.2 All Payment Devices remain our property

Should you request a Payment Device be linked to your Card account, we may charge you a fee for the manufacture, use and set up of the Payment Device which will be described in the relevant Credit Card Schedule.

All Payment Devices remain our property at all times until such time as:

- you request us to cancel your use of the Payment Device;
- you close your Card account that the Payment Device is linked to;
- expiry of the Payment Device;
- expiry of the Card account that the Payment Device is linked to; or
- electronic access to your Card account has been cancelled in accordance with clause 1.5.

Notwithstanding the above, we retain the right to terminate a user's licence to use the Payment Device at any time. If we exercise this right within one year from the date that a user's Payment Device was first issued and do not replace the Payment Device, we will give you a pro-rata refund of any fee paid for the Payment Device.

8.3 Use of the Payment Device

In order to use a Payment Device, you must have activated the linked Card in respect of the Card account. You can activate a Card by following the directions that we will provide for that purpose.

The Payment Device is valid only for the period of the linked Card. On expiry, you will need to request the issue of a further Payment Device and pay any applicable Payment Device fee.

If a Payment Device is used outside Australia, all charges, purchases and/or cash advances in foreign currency are converted, from foreign currency to Australian currency by Mastercard International Incorporated at a wholesale exchange rate selected by Mastercard International Incorporated on the processing date, which rate may differ from the rate applicable to the date the transaction occurred and that applicable to the date the transaction was posted. For all transactions effected by a foreign currency or transactions occurring outside Australia (whether effected in foreign currency or Australian dollars) or while you are in Australia (for example, online) where the merchant or the financial institution or entity processing the transaction, is located overseas, we will charge the Foreign Transaction Fee as described in the Financial Table of the Credit Card Schedule.

8.4 Types of transactions that can be made

Purchases of an amount up to the contactless payment threshold can be performed by using the Payment Device and making contactless payments at merchant terminals. For purchases above the contactless payment threshold, a user must 'tap' their Payment Device on the merchant terminal and enter their PIN to complete the transaction. The user should make sure the correct transaction details are displayed on the merchant terminal and wait for the transaction confirmation.

No other transactions are permitted using the Payment Device.

8.5 Transactions needing authorisation

Transactions on the Card account that the Payment Device is linked to may need to be authorised by us. We may decline to authorise a transaction if:

- you are behind in making payments to that Card account;
- the credit limit on the Card account is exceeded; or
- there is good reason to do so (including security reasons).

If you, or the merchant, do not proceed with a transaction after it has been authorised by us your available balance may be reduced for at least seven business days.

8.6 Transactions at EFT Terminals

When a user makes an EFT transaction at an EFT terminal using the Payment Device and PIN or Payment Device and contactless payment you authorise us to act on the instructions entered into the EFT terminal. Users should make sure that the correct details are entered into the EFT terminal before authorising a transaction and 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 Card account that the Payment Device is linked to on the day they are made. Processing may take a number of days. We will process transactions to your Card account as soon as practicable after receipt.

You should observe the guidelines set out in Part 7 of these Conditions of Use to ensure the security of your access method when transacting at an EFT terminal.

8.7 Use of a Payment Device at merchants, financial institutions or our agents

To the extent permitted by law and the ePayments Code we do not accept responsibility for the actions of a merchant, financial institution or our agent who:

– refuses to honour a Payment Device; or
– imposes limits or conditions on use of a Payment Device.

Unless required by law we will not be liable for goods or services supplied using a Payment Device. Users 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 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.

We have no control over and take no responsibility for the hours a merchant, financial institution or our agents may be open for business. Times when an EFT terminal is available will depend on

the opening hours of the relevant merchant, financial institution or agent.

If you provide a merchant with your Payment Device details (by tapping your Payment Device at a merchant terminal):

- to enable the merchant to complete a transaction in the future (e.g. authorises a public transport provider for additional rides in the day); or
- to pay for goods and services in advance even if you later decide not to take the good or use the services;

You authorise the merchant to complete the transaction.

8.8 Payment Devices

The Australian Consumer Law provides for certain warranties in relation to products and services, including Payment Devices. For example, you are entitled to a replacement or refund of any Payment Device fee where the Payment Device is faulty. You are also entitled to have the Payment Device repaired or replaced if it is not of an acceptable quality. Should we be unable to issue you with a Payment Device, we will refund any relevant fee. We warrant that the Payment Device will be free from defects in material and workmanship under normal use for period is which the Payment Device is valid. We are not responsible for damage arising from failure to follow the instructions relating to the use of the Payment Device.

To the extent permitted by applicable law, including the Australian Consumer Law:

- other than to the extent that we or our representatives have made a representation on which it is reasonable for you to rely we do not make any express or implied warranty or representation in connection with the Payment Device (including type, quality or standard of fitness for any purpose);
- other than to the extent that we or our representatives have made a representation on which it is reasonable for you to rely do not make any express or implied warranty as to the reliability of any software or hardware elements which when assembled represent the Payment Device; and
- are not liable for any loss you suffer (including any direct or consequential loss) arising in connection with the Payment Device (whether due to a failure to provide the Payment Device or its loss, theft or destruction), other than to the extent that the loss is directly caused by our act or omission.

Part 9 – Procedures For Handling Errors and Disputed Transactions

The entirety of Part 9 applies to unauthorised transactions and disputed transactions (chargebacks), and reflects our obligations under the ePayments Code.

Clauses 9.1 – 9.3 do not apply to:

- *general complaints (including complaints about compliance with the ePayments Code) - please see the Banking Services Rights and Obligations booklet (available on the Bankwest website) for information about how to make general complaints;*
- *reports of Mistaken Internet Payments under the ePayments Code, which have a separate process set out in clause 4.10. For how to report a Mistaken Internet Payment, see clause 4.10(c). If you have a complaint regarding how we or a Receiving ADI have handled a report of a Mistaken Internet Payment, it will be addressed as per the Banking Services Rights and Obligations booklet (available on the Bankwest website).*

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

If you believe an entry on your Card Account statement is wrong or unauthorised, you should promptly tell us by:

- using the Bankwest App;
- messaging us in Online Banking;
- following the procedure set out on our website; or
- telephoning us.

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

- your name, address, credit card number and account details;
- 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 matter.

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 Payments. 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 Additional 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 your Card account (see Clause 3.14 (t)). 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 within 14 days of the date of the account statement 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.

In certain circumstances where the ePayments Code applies, there may be no such timeframes imposed upon your right to make a claim or report a disputed transaction.

9.1.1 If we are unable to resolve the matter within 5 business days to both your and our satisfaction we will advise you in writing of our procedures for further investigation and handling of your matter.

9.1.2 Within 21 days of you reporting your matter to us (or, if we resolve your matter by exercising our rights under the Mastercard

scheme rules, within the time period specified in those rules), 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 (or, if we resolve your matter by exercising our rights under the Mastercard scheme rules, within 60 days) of you reporting your matter to us, unless there are exceptional circumstances.

9.1.3 Subject to Clause 9.1.4, if we are unable to resolve your matter 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.

9.1.4 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 9.1.2;
– comply with Clause 9.1.3 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.

9.2 Outcome

If required under the ePayments Code, 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 Credit Card Account Access Conditions of Use and the ePayments Code. If we decide that your 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 a disputed transaction, we will supply you with copies of any document or other evidence on which we base our findings if these show that your 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.

9.3 If you are not satisfied

If you are not satisfied with our findings or have a complaint or dispute, you may request our Customer Relations Department to review the matter. Contact them by writing to:

Manager Customer Care
GPO Box E237
Perth WA 6841

or phone to:

Telephone: Freecall 1800 650 111

Additionally, you may be able to refer the matter (free of charge) to:

Australian Financial Complaints Authority
GPO Box 3
Melbourne VIC 3001

Telephone: 1800 931 678
Website: www.afca.org.au

Email: info@afca.org.au

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

9.4 If we fail to comply with these procedures

If we fail to observe the procedures set out in this clause or the ePayments Code for handling disputes, allocating liability or communicating the reasons for our decision and that failure contributes to our decision or delays the resolution of your matter, we may be liable for part or all of the amount of a disputed transaction.

Part 10 – Privacy

(a) We may collect personal information about you or a User (including any mobile device of you or 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 our Privacy Statement.

(b) We may disclose personal and transactional information (including any mobile device of you or 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), or in order to investigate a Mistaken Internet Payment, including:

  i. any party nominated to receive a payment;

  ii. BPAY Pty Ltd and any agent appointed to 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; and

  v. a Receiving ADI or unintended recipient in relation to a Mistaken Internet Payment.

(c) Users may have access to the personal information we hold about them at any time by asking us. Where that personal information is incorrect, Users may have their personal information corrected.

(d) You 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 your personal information, please refer to our Privacy Statement, available from our website **bankwest.com.au** or by telephoning us.

This page has intentionally been left blank

bankwest.com.au

BWA-8105 060625

6 June 2025