bankwest

# Account Access.

Conditions of use

# Product Disclosure Statement

If you are opening a Bankwest-branded Investment and Transaction Account with us, or are applying for Bankwest Online Banking, Phone Banking, a Payment Device or a Bankwest Debit Card (including a Debit Mastercard) for use in connection with an Investment and Transaction Account that you already hold, these Terms and Conditions will form part of the Bank's Product Disclosure Statement (PDS) for the relevant product(s) and must be read together with the other components of that PDS.

You will also be given:

The Investment and Transaction Accounts Terms and Conditions, a Product Schedule, the Banking Services Rights and Obligations brochure, and the Your Guide to Banking Fees brochure.

You should read all of these documents carefully and retain them for future reference. Copies of each of the documents can be made available to you on request from our Contact Centre or can be viewed on our website bankwest.com.au.

**Enquiries:** Message Us in the Bankwest App or contact the Customer Contact Centre 13 17 19

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.

# Contents

# About these Conditions of Use

These Conditions of Use apply to your use of the following Bankwest Services if the Product Schedule for your nominated account states that the Service is available to you.

- Bankwest Online Banking* – Parts 1, 4, 7, 8 and 11
- Phone Banking* – Parts 1, 4, 7, 8 and 11
- PayAnyBody – Parts 1, 4, 5, 7, 8 and 11
- Payment Devices – Parts 1, 7, 8 and 11
- PayTo – Parts 1, 4, 7, 8, 11 and 12
- Bankwest Debit Cards (excluding Debit Mastercards) – Parts 1, 2, 7, 8 and 11
- Debit Mastercards – Parts 1, 3, 6, 7, 8, 9 and 11

These Conditions of Use also apply when we share your information with other parties under Confirmation of Payee.

Each of these Services provides you with access to Bankwest accounts which we agree you may nominate.

The Bank's credit card products are governed by separate conditions unique to those credit card products – the Credit Card Account Access Conditions of Use and the Credit Card Conditions of Use. Those conditions govern the use of the credit card to access the credit card account. However, where you have a credit card linked to a nominated cheque or savings account, the use of the credit card to access that account will be governed by these Account Access Conditions of Use and not by the Credit Card Account Access Conditions of Use.

Before you use any of the above Bankwest Services you should read these Conditions of Use carefully. They operate in addition to and should be read together with the Conditions of Use applying to your nominated accounts. If there is an inconsistency between these Conditions of Use and the Conditions of Use applying to your nominated account, these Conditions of Use prevail in respect of:

- EFT transactions,
- transactions effected with Debit Mastercard where a manual signature is the principal means of verifying the authority to give the instruction;
- transactions effected with a card (including Debit Mastercard) with Contactless payments; and
- transactions effected using a Payment Device to make payments.

*Including the BPAY scheme

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.

You should keep these Conditions of Use for future reference. Copies of the Conditions of Use are available on our website (bankwest.com.au).

**Customer Enquiries – Message Us in the Bankwest App or contact the Contact Centre 13 17 19**

**Where to report Lost or Stolen Cards, Payment Devices or Suspected Unauthorised Transactions (24 hours)**

**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).

Part 1

# General Conditions of Use

## 1.1 Definitions

The following expressions have the following meaning:

**Access method** means a method the use of which we authorise and accept as providing authority to us to act on an instruction given through electronic equipment.

A reference to an access method includes a reference to each of its individual components and includes, but is not limited to, a card, card details, a security token, a mobile device, a Mobile Wallet, a Biometric Identifier, a secret code, 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 instruction.

**Account Holder (Online Banking)** means the legal owner of a Nominated Account.

**Additional cardholder** means a person who has been nominated by you and authorised by us to operate your nominated accounts alone.

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

**ATM** means an automatic teller machine.

**Biller** means an organisation who tells you that you can make bill payments to them through the BPAY® scheme.

**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 a transaction.

**BPAY Group Ltd** means BPAY Group Ltd ABN 60 003 311 644 (previously known as Cardlink Services Ltd) PO Box H124 Australia Square NSW 1215.
Tel: (02) 9646 9222.

**BPAY payment** means a payment to a biller through the BPAY scheme (excluding Osko Payments and other Faster Payments).

**BPAY Group Ltd** means BPAY Group Ltd ABN 69 079 137 518 (previously known as Cardlink Services Ltd) PO Box H124 Australia Square NSW 1215
Tel: (02) 9646 9222.

**BPAY Pty Ltd** means BPAY Pty Ltd ABN 69 079 137 518, GPO Box H124 Australia Square NSW 1215.
Tel: (02) 9646 9222.

**BPAY scheme or BPAY** means a service which allows you to (a) make BPAY payments electronically and (b) make Osko Payments.

We have membership of the BPAY scheme. We will tell you if we cease to have membership of the BPAY scheme.

**Business day** means any weekday, including local public holidays in Australia, but excluding public holidays observed Australia wide.

**Card** means a Bankwest-branded card issued by us to enable you to access your nominated accounts, including:

- a Debit Mastercard (except in Part 2, where a reference to a card does not include a reference to a Debit Mastercard) with any embedded electronic microchip; a Virtual Card and
- a credit card used to access a cheque or savings account (but excluding a credit card used to access a credit card account).

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

**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.

**Contactless payments** means authorising a transaction of an amount up to the Contactless payment threshold by tapping your card or Payment Device on a merchant terminal. You do not have to sign or enter a PIN.

**Daily Payment Limit (Online Business Banking)** means the aggregate amount of Payments that you may instruct us via Online Business Banking to make from your Nominated Accounts on any Business Day, which is currently $50,000.00, or an amount we advise or agree with you.

**Direct Debit** has the meaning given to the term 'Direct Debit Request" in the BECS Procedures available at https://www.auspaynet.com.au/resources/direct-entry

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

**EFT system** means the shared system under which EFT transactions are processed.

® Registered to BPAY Pty Ltd ABN 69 079 137 518

**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.

**EFT transaction** means an electronic funds transfer from or to a Bankwest-branded account with us initiated by a user through electronic equipment using an access method.

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

**Electronic communication** means a message we transmit to you and you receive from us electronically, in a form that you can retain for later reference such as by printing or by storing for later display or listening; Electronic equipment includes, but is not limited to, a computer, television, telephone, mobile phone, mobile devices and an EFT terminal.

**Eligible Account (Online Business Banking)** means a Bankwest-branded account of a type that Bankwest determines from time to time is eligible to be accessed via Online Business Banking.

**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.

**Error Payment** means Faster Payment initiated by a User in circumstances where the ePayments Code does not apply and which, as a result of the User's error, is directed to the wrong account. Error Payments are excluded from the procedure set out in 5.16 ("Mistakes as to the account to which a Pay AnyBody payment is made").

**Faster Payment** means, as relevant:

- an NPP Payment; or
- a payment to a PayID, or to a BSB/account number, that is settled within the Commonwealth Bank of Australia group.

**Faster Payment Over Payment** means a correctly directed Faster Payment where the amount has been submitted for an amount greater than intended by the User or for an amount that exceeds the payment due.

**Faster Payment Repeated in Error** means a correctly directed Faster Payment which has been inadvertently made more than once by a User.

**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.

**First Time Payment** means the first payment to a payee who, at the time of that payment, is not on your list of saved recipients, and also includes all subsequent payments to that payee made within 48 hours after the first payment.

**Instruction (Online Business Banking)** means any request or instruction to Bankwest that is effected through Online Business Banking by use of a PAN and Password.

**International transfer** means a payment to a beneficiary account at a bank overseas.

**Mandate Management Service** means the central, secure database operated by NPP Australia Limited of Payment Agreements.

**Mastercard® scheme rules** means the credit card rules of Mastercard International Incorporated, which apply to all transactions effected with the Debit Mastercard or Payment Device (other than those made by selecting the Cheque or Savings key at an EFT Terminal, or any transactions otherwise routed through the EFTPOS card scheme).

**Merchant** means a supplier of goods or services including, where relevant, a supplier with which you have established, or would like to establish, a Payment Agreement.

**Migrated DDR Mandates** has the meaning given in clause 12.7.

**Misdirected Payment** means a Faster Payment erroneously directed to an incorrect account because the financial institution that registered the PayID has not correctly registered or maintained the correct information.

**Mistaken Internet Payment** means a payment initiated using the Pay Anybody service (including a Faster Payment) described in clause 5.2 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, or PayID 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, or PayID.

This does not include payments made using BPAY or the PayTo Service.

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

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

**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.

NameCheck 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.

**Nominated account** means a Bankwest-branded account with us, other than a credit card account, which you nominate and which we authorise you to:

- access to conduct EFT transactions; and/or
- access with a Debit Mastercard where a manual signature is the principal means of verifying the authority to give the instruction.

If there is more than one account holder and/or more than one authorised signatory to the account, each account holder and each signatory must be authorised to operate the nominated account alone;

**Nominated Account (Online Business Banking)** means an Eligible Account you operate with Bankwest that you nominate to be accessed, in order to transfer funds to or from it or obtain information about it, by using Online Business Banking. This includes, without limitation, an individual account, joint account, company account, trust account or a partnership account provided that if the account allows for more than one signatory to effect transactions in respect of it, the account operation method requires Instructions to be given by "any one" of a number of signatories or by "any two of them jointly".

**NPP** means the New Payment Platform.

**NPP Payment** means a Pay Anybody payment that is cleared and settled via the NPP (and includes Osko Payments and payments made through the PayTo Service).

**NPP Procedures** means the procedures relating to the NPP with which industry participants in the NPP (including Bankwest) must comply.

**Online Business Banking means** Bankwest's Online Business Banking Internet service, which allows you to conduct your business banking and transact online on your Nominated Accounts. It also includes such other electronic or computer-based banking services that Bankwest may add to the service from time to time. With the exception of international transfers, which are governed by these Account Access Conditions of Use and the Your Guide to Banking Fees Brochure, the Online Business Banking Product Disclosure Statement governs Bankwest Online Business Banking.

**Osko** means the Osko payment service provided by BPAY Pty Ltd.

**Osko Payment** means an NPP Payment made through Bankwest Online Banking using Osko. The following payments are not eligible to be Osko Payments:

a) international payments

b) phone banking payments

c) payments where the payee's financial institution is not a participant in Osko or the NPP

d) payments where the payee's account is not eligible to receive Osko Payments

e) payments to a PayID where the payee has not registered a PayID with the payee's financial institution

f) payments outside any transaction limits applying to Osko Payments from time to time

g) (unless we tell you) future-dated transfers

h) (unless we tell you) scheduled payments (e.g. weekly or monthly payments)

**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 ten-digit code which is a combination of the token PIN and token code.

**PayID** means a smart address for Faster Payments (including Osko Payments and payments made through the PayTo Service), composed of a PayID Type linked to a nominated account.

**PayID Name** means the name we give you to identify and register you in the PayID Service.

**PayID Service** means the smart payment addressing service for sending and receiving Faster Payments (including Osko Payments and payments made through the PayTo Service).

**PayID Type** means a piece of recognisable and memorable information that can be linked to a financial account (including a nominated account) to create a PayID. PayID types include phone number, email address, Australian Business Numbers and other organisational identifications. We will let you know what PayID Type/s we will accept to link to an account

**Payment (Online Business Banking)** means a transfer of value (including an internal transfer) from a Nominated Account to: other Nominated Accounts (provided that the payment does not involve a transfer between two credit card accounts), any other Bankwest-branded accounts (whether of the Account Holder or any other persons) or NonBankwest branded accounts (whether of the Account Holder or any other persons), except credit card accounts.

**Payment Agreement** means an agreement established by you and an approved Merchant or Payment Initiator, by which you authorise us to make payments from your PayTo Account.

**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 nominated account.

*Effective 28 September 2021 the Bankwest Halo payment device is withdrawn from sale. Customers who already hold a Bankwest Halo payment device can continue using it until the expiry date of the device, however from 1 December 2021 the Bank will no longer reissue or replace any existing Bankwest Halo payment device

**Payment Initiator** means an approved payment service provider who, whether acting on behalf of you or a Merchant, is authorised by you to initiate payments from your PayTo Account.

**PayTo Account** means your Bankwest-branded account with us that we agree may be nominated by you to be debited under a Payment Agreement.

**PayTo Service** means the service which enables us to process NPP Payments from your PayTo Account in accordance with and on the terms set out in a Payment Agreement you have established with a Merchant or Payment Initiator that subscribes to the service.

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

**Privacy Law** means The Privacy Act 1988 (Cth) and regulations made under that Act.

**Product Schedule** means the Product Schedule for the relevant Service or nominated account.

**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 where 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 prearranged 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 Debit Mastercard with merchants that take part in the 'Mastercard SecureCode' or 'eftpos Secure' 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** is Bankwest's Online Banking, Phone Banking, Pay Anybody, Payment Device, Debit Card (including Debit Mastercard), or PayTo Service, as relevant.

**SMS Code** means a randomly generated 6 digit code we send by short messaging service (SMS) to your mobile phone for conducting certain Secured Online Shopping transactions using your card (not including a card referred to in Part 2) 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 a person other than the user.

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

**Transfer ID** means a unique identification number generated by the Mandate Management Service in connection with a request to transfer one or more Payment Agreements.

**Unauthorised** means without the knowledge or consent of a user.

**User** means you and any additional cardholder (if relevant), and any other person authorised by you and us to operate a nominated account alone (i.e. an authorised signatory).

**Virtual Card** means a type of Card that:

- may be provided to you via a request made through the Bankwest App;
- that exists solely in virtual (digital) form (ie a Virtual Card is not available in physical form);
- uses Debit Mastercard payment infrastructure;
- contains Card details not replicated on any other Debit Mastercard issued in connection with a nominated account; and
- may be used either on a single-use basis, or a multi-use basis (see Part 3 of these 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 nominated account and each of you if there is more than one account holder. Any other grammatical form of the word 'you' has a corresponding meaning. For the purposes of complying with the requirements for the SMS Code Security and the Secret Questions Security, where relevant, "you" also includes any user. Unless otherwise required by the context, a singular word includes the plural and vice versa.

## 1.2 ePayments Code

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

## 1.3 Banking Code of Practice

The Banking Code of Practice applies to the Services. General descriptive information about our banking services is available on request in the form of a booklet issued by us called Banking Services Rights and Obligations. It includes, in particular, information about account opening procedures, our obligations regarding the confidentiality of your information, our complaint handling procedures, bank cheques, and on the advisability of you reading the terms and conditions applying to our banking services and of informing us promptly when you are in financial difficulty.

## 1.4 Acceptance

The first use of an access method (or the first use of the Debit Mastercard where a manual signature is given to verify the authority to give the instruction) after receiving these Conditions of Use will constitute your agreement to the Conditions of Use in respect of the Service which is accessed.

## 1.5 Statements

Statements of account for nominated accounts will be sent as frequently as required by the terms and conditions applying to the nominated account, by law or as you have requested.

In any event, statements of account for nominated accounts will be sent at least every six months, but there may be circumstances where we are not able to do so (such as where you have not provided us with your new address or particulars).

You may also request a statement at any time. You should check all entries on statements for nominated accounts and tell us promptly of any error or possible unauthorised transaction.

Statements of account may be sent electronically, in accordance with clause 1.8.

For paper statements, a Paper Statement Fee may apply.

## 1.6 Fees and charges

For fees and charges applicable to the issue or use of an access method, refer to the relevant Product Schedule(s) message us in the Bankwest App or contact our Contact Centre.

We will debit your nominated accounts with any fees and charges incurred in the issue or use of an access method and with all duties, taxes and charges which governments may impose on us or you due to electronic transactions on your nominated accounts or to the provision of any of the Services. These government duties may include state debit tax.

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.

## 1.7 Changes to these Conditions of Use

**Changes by us**

We can change any of these Conditions of Use at any time. Circumstances where we may make changes to the terms and conditions include, but are not limited to, those where there are:

- changes to the cost of providing the account or services to you;
- changes in legal or other regulatory requirements affecting us;
- changes in any system or product development or enhancement.

If you consider that you will be adversely affected by changes notified to you under this clause, you may end your use of a Service or contact us to close the account.

We will give you at least 30 days (or such longer period required by law) written notice of a change which:

- imposes or increases charges relating solely to the use of an access method or the issue of an additional or replacement access method;
- increases your liability for losses relating to EFT transactions; or
- imposes, removes or adjusts a daily or other periodic transaction limit applying to the use of an access method, a nominated 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 a nominated account, including the prevention of system or individual criminal activity, including fraud and scams, we may make a change necessary for that purpose without giving you advance notice.

We may notify you of changes by:

- the electronic means described in clause 1.8;
- a notice on or with your nominated account statement;
- publishing a press advertisement; or
- 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 contacting the Contact Centre.

## 1.8 Electronic communications with you

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 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, or your nominated account signatory on a business account, can:

- elect not to receive information by electronic communication; and
- change the nominated address (including electronic address) for receiving notices, including statements.

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) and other personal information, 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.

## 1.9 Cancellation of access

a) We may in our discretion, to you:

- withdraw or deny access to a Service (including Faster Payments),
- 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 nominated 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 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 your transaction instructions are not clear;

- if we reasonably consider there has been non-compliance with these 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 sanctio\ ned jurisdiction (while the User is in that jurisdiction). To find out the current list of sanctioned jurisdictions please visit commbank.com.au/sanctionedcountries (this list may change from time to time without notice to you).
- if we suspect on reasonable grounds that your account is being used in a way that results in or may cause financial abuse

Except to the extent we act negligently in taking any action under this clause, 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 nominated account.

b) We may suspend or limit electronic access to your nominated account at any time without notice if, in our reasonable opinion:
   - you have not complied with the requirements for your Security Setting; or
   - we consider a security issue has arisen which requires further investigation.

c) You may end your use of a Service or cancel a user's electronic access to your nominated account at any time by messaging us in the Bankwest App or contacting the Contact Centre.

d) Notwithstanding clause 1.9 (a), (b) or (c), we may cancel your use of a Service at any time on providing reasonable notice to you.

When electronic access to your nominated account has been cancelled by you or us, you must (if relevant):

- halt the use of any card, Payment Device 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
- ensure that any security token is returned to us undamaged.

The Bank has an obligation under the Banking Code of Practice to act fairly and reasonably towards you in a consistent and ethical manner.

## 1.10 Contact

You can contact us by:

- messaging us in the Bankwest App; or
- phoning our Contact Centre; or
- writing to us at GPO Box E237, Perth, Western Australia, 6841; or
- sending a message to us using the secured e-mail facility available within Bankwest Online Banking.

## 1.11 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 Policy

b) We may disclose personal and transactional information (including information about 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 NPP and / or the BPAY scheme) or in order to investigate a payment made in connection with the PayTo Service or a Mistaken Internet Payment, including:

iii) any party nominated to receive a payment;

iv) BPAY Pty Ltd and any agent appointed to it from time to time, including BPay Group Ltd who

provides the electronic systems to implement parts of the BPAY scheme;

v) any party we may use in sending SMS Code to you;

vi) agents and contractors we may use in providing any of our Services; and

vii) 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.

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

e) You can request access to information held by BPAY Pty Ltd or its agent BPay Group Ltd using the contact details supplied in clause 1.1.

f) You agree and consent to any use and disclosure of your personal information for the above purposes, even if the disclosure is to an organisation overseas and that organisation is not subject to the same privacy obligations that apply to us. You acknowledge that:

i) in most cases, you will, upon request, be able to access and correct any personal information we hold about you subject to the payment of any fee we may charge; and

ii) in the absence of your consent to the use and disclosure of your personal information for the above purposes, we cannot act on your payment instructions (including instructions in respect of BPAY payments, Faster Payments and Osko Payments).

g) You agree that, if you supply us with personal information about another individual (for example about a User or information which identifies a person to whom a payment or Direct Debit is directed), you will advise that individual of the content of this clause and tell him or her that:

– We have been provided with and are holding personal information about that person and that he or she can contact our Contact Centre;

– The personal information collected about that person will be used for the purposes set out above in this clause and that, without that information, these purposes could not be fulfilled;

– The personal information collected about that person will usually be disclosed in the manner set out above in this clause; and

– That person has the right to access and correct the personal information we hold about him or her.

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

## 1.12 Confirmation of Payee

Confirmation of Payee is a service that:

– may be provided to a payer by their financial institution; and

– may allow the payer to confirm the account name of the BSB and account number they want to make a payment to.

We will endeavour to ensure your account details are accurately recorded by us for the purposes of the use of the Confirmation of Payee service. You acknowledge and authorise:

– us to use and disclose your account details as part of Confirmation of Payee; and

– payers' financial institutions to use your account details for the purposes of Confirmation of Payee and prior to making payments to you.

To the extent your account details and the use of your account details as part of Confirmation of Payee constitutes disclosure, storage and use of your personal information within the meaning of the Privacy Law, you acknowledge and agree that you consent to that disclosure, storage and use.

At our discretion we may permit you to opt-out of Confirmation of Payee in very limited circumstances. Please contact us if you wish to opt-out of Confirmation of Payee.

In the event that we accept your request to opt-out of Confirmation of Payee, you nonetheless acknowledge and authorise us to confirm, disclose, store and use your account details through the Confirmation of Payee service to government agencies for the purposes of government agencies making payments to you.

You may provide alternative names to be recorded on your account for the purposes of Confirmation of Payee in some circumstances. Please contact us if you wish to do so.

## 1.13 Consumer Data Right

You can share certain data that relates to you with accredited third parties under the Consumer Data Right **(CDR)**. The CDR was introduced by the Federal Government to provide customers with rights to access specified data that relates to them **(CDR data)** held by organisations **(data holders)**; and allow them to authorise the sharing of that CDR data to other

third parties **(accredited data recipients)**. For more information about the CDR, please see our Consumer Data Right Policy available on our website at bankwest.com.au.

Our Consumer Data Right Policy describes your rights under the CDR legislation.

For joint account holders, our Consumer Data Right Policy includes information about the circumstances in which you or any of your other account holders is able to:

- share data from your joint account with accredited data recipients under the CDR, without each other's further approval; or
- choose another person as a data sharing delegate without each other's approval. A data sharing delegate is able to share data from your joint account with accredited data recipients without further approval.

## 1.14 Severance

If any part or provision of the Conditions of Use is or becomes void or unenforceable under any applicable statute in any State or Territory then as to that State or Territory that part or provision will be removed from the Conditions of Use. Removal of any part or provision will not affect the remaining provisions in that State or Territory or affect the validity or enforceability of that part or provision in any other State or Territory.

## 1.15 Your Security Setting

Your Security Setting provides additional security where you wish to register and manage a PayID and/or 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 Conditions of Use, all users must be registered for SMS Code Security when required by us. All users must notify us of their current mobile phone number and inform us of any change in their mobile phone number by contacting us in accordance with clause 1.10.

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 Conditions of Use, all users of Bankwest Online Banking must be registered for SMS Code Security and Secret Questions Security when required by us.

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

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

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

We may suspend your SMS Code Security if we have reason to believe that your online security, or card 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 , and/or your ability to use a card at online merchants, may be suspended or limited and will not apply until we reactivate it. Call the Contact Centre.

## 1.16 Exercising discretion

If any provision of the Conditions of Use contemplates that we would exercise a discretion to approve, agree to or consent to any matter, that provision shall be interpreted so as to require us to act reasonably in the exercise of our discretion and in accordance with our legitimate interests.

## 1.17 Other limits

In addition to any other limit which may apply to transactions to which these Conditions of Use apply, we may in our discretion, limit the amount each user may transfer or pay from all your Bankwest accounts:

- using Services to accounts and/or merchants which we reasonably believe may be owned or controlled by a crypto-currency or digital asset exchange, or being used to purchase crypto-currency or digital assets, to no more than AUD $10,000 in a calendar month; and/orusing a particular Service or dealing to no more than AUD $10,000 in a calendar month; and/or
- using Services where it is reasonably necessary to prevent systemic or individual criminal activity including suspected or potential fraud or scams, to no more than AUD $10,000 in a calendar month.

Except to the extent that we act negligently in taking any action under this clause, we will not be responsible for any loss, cost, expense or other inconvenience you incur.

Part 2

# Debit Cards Conditions of Use

## 2.1 About these conditions

Part 2 (together with Parts 1, 7, 8 and 11) of these Conditions of Use applies to all transactions involving the use of a card (other than a Debit Mastercard).

All references in this Part to "nominated account" are taken to include a reference to "Nominated Account".

## 2.2 All cards remain our property

All cards remain our property at all times.

You agree to return all cards to us:

- on request by us;
- when you close your nominated account; or
- when electronic access to your nominated account has been cancelled in accordance with clause 1.9.

## 2.3 Additional cardholder

If your nominated account permits, you may request us in writing to issue a card and PIN to an additional cardholder.

The relevant provisions of these Conditions of Use apply to the additional cardholder's use of the card (including their use of the card online and use of the card with a PIN), to access your nominated account. You are responsible for informing the additional cardholder how to use the card and PIN. We suggest that you provide the additional cardholder with a copy of these Conditions of Use.

You and not the additional cardholder will be liable for all transactions made by the additional cardholder on your nominated account using the card until the additional cardholder's authority is cancelled.

An additional cardholder's authority is cancelled only when:

- we have received your request to cancel that person's card; and
- that card has been returned to us for cancellation, or we are satisfied, acting reasonably, either that the card has been destroyed or that you have taken all reasonable steps to procure its return to us.

It is your responsibility to ensure that the additional cardholder's card is returned to us. You consent to the additional cardholder having access, in respect of nominated accounts, to information about the account balance, payments, purchases and cash advances.

## 2.4 Use of the card

The card is valid only for the period (if any) indicated on it. The card must be signed as soon as it is received.

The card must be destroyed by cutting it in half diagonally and through the card details and any electronic microchip when it has expired or otherwise ceased to be valid.

## 2.5 Types of transactions that can be made

The following transactions can be performed by using the card with PIN to access a nominated account:

- withdrawals;
- purchases;
- transfers;
- deposits;
- obtain the balance on a nominated account; and
- request a statement.

When you are advised of the availability of Contactless payments on your card, purchases of an amount up to the Contactless payment threshold can also be performed by using the card and Contactless payments at merchant terminals. When you are advised of the availability of this function, the card may also be used without a PIN to make purchases at selected online merchants.

Not all types of transactions apply to all nominated accounts. It may not be possible to use all EFT terminals to carry out applicable transactions on nominated accounts. Not all merchants will permit the use of a card to make purchases online.

For further information call our Contact Centre.

## 2.6 Where the card with PIN can be used

Users can use the card with PIN:

- at any ATM or EFTPOS in Australia;
- at selected agents.

### 2.6a Where the card and Contactless payments can be used

Users with a card with a EMVCo Contactless Indicator on the front of the card can perform Contactless payments transaction. To make a purchase using Contactless, 'tap' your card on the merchant terminal and wait for the transaction confirmation. You should make sure the correct transaction details are displayed on the merchant terminal and you should not generally need to hand your card over to the merchant, sign or enter a PIN to complete the transaction. You can also use your card with Contactless payments anywhere EMVCo Contactless Indicator is displayed. You can still enter a PIN at EFT terminals or provide a signature in some cases depending on your card, even if your card is enabled with Contactless payments.

### 2.6b Where the card can be used with a Mobile Wallet

A card with an electronic microchip may be used with a Mobile Wallet we approve for use from time to time to make Contactless payments to retailers and payments within Mobile Wallet applications.

If the dollar value of a 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 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 a 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 a 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 Debit Mastercard 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.

It may be possible to make 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. 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;
- we suspect on reasonable grounds that your account is being used in a way that results in or may cause financial abuse.
- 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 Account Access Conditions of Use or the terms and conditions specific to the account.

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

## 2.7 Daily transaction limits

a) At ATMs

The minimum amount users can withdraw each day from CommBank ATMs is $20 or $50 (depending on the ATM). A maximum daily transaction limit also applies. Users will be advised of this limit when their card is issued. The minimum and maximum cash withdrawal limits applying to non-CommBank ATMs may vary.

b) Our agents and EFTPOS terminals

The maximum aggregate amount that can be withdrawn daily from our agents that provide withdrawal services and when making purchases from EFTPOS merchants using a card and PIN, or when making online purchases using the card, is the maximum daily transaction limit. Merchants, our agents, non-Bankwest-branded outlets, and other financial institutions may have additional restrictions on the amount of funds that may be withdrawn, paid or transferred.

## 2.8 Depositing funds using the card with PIN

You can deposit funds to your nominated account at selected agents and select CommBank ATMs. There are limits on the amount of cash you can deposit at our agents and at ATMs (see the Bankwest website for details). If a cheque (other than a foreign cheque, in any currency) is deposited to the account, the amount of the cheque will be credited on the business day it is received by us but it will not be available to you until it is cleared. Effective immediately in relation to all accounts opened on or after 3 October 2022, and on and from 31 March 2023 in relation to all other accounts, you may not deposit foreign cheques (in any currency) to your account. All deposits made at CommBank ATMs are checked by us. If the amount appearing on the transaction record differs from the amount actually received by us, we will credit your nominated account with the amount actually received and notify you as soon as possible.

## 2.9 Transactions needing authorisation

Transactions on nominated accounts may need to be authorised by us. We may decline to authorise a transaction if:

- you are behind in making payments to a nominated account;
- the credit limit on a nominated account would be exceeded;
- there are insufficient funds in a cheque or savings nominated account; or
- there is good reason to do so (including security reasons).

## 2.10 Transactions at EFT terminals

When a user makes an EFT transaction at an EFT terminal using the card and PIN , or card 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 nominated accounts on the day they are made. Processing may take a number of days. We will process transactions to your nominated accounts as soon as practicable after receipt.

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 via EFT terminal, 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.

**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.**

## 2.11 Use of a card 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 or financial institution who:

– refuses to honour a card; or

– imposes limits or conditions on use of a card.

Card promotional material and material promoting EFTPOS displayed on the physical premises, or online stores, of merchants, financial institutions and our agents is not a warranty by us that card and EFTPOS facilities are available or that goods and services may be purchased using the card.

Unless required by law we will not be liable for goods or services supplied using a card. Users must take up any complaints or concerns directly with the merchant and any refund is a matter between the user and the merchant.

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 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 you later decide not to take the goods or use the services, you authorise the merchant to complete the transaction.

## 2.12 Use of card at online merchants

A user will be advised by an online merchant if a card may be used to make purchases at the online merchant.

Users under 16 years of age are not permitted to use a card to make a purchase at an online merchant. When a user makes a purchase using a card at an online merchant, the purchase will be processed as a “Savings” transaction unless:

– the online merchant provides the user with the option to have the purchase processed as a “Cheque” transaction and the users chooses the “Cheque” option; or

– the nominated account linked to the card is a “Cheque” account (and not a “Savings” account). In which case, the purchase will be processed as a “Cheque” transaction.

An electronic withdrawal fee may apply to the use of a card to make a purchase at an online merchant.

## 2.13 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 1.9(a) (“Cancellation of 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

# Debit Mastercard and Virtual Cards Conditions of Use

## 3.1 About these conditions

Part 3 (together with Parts 1, 7, 8, 9 and 11) of these Conditions of Use applies to all transactions involving the use of:

- the Debit Mastercard and PIN, or Virtual Card Card details. at EFT terminals;
- the Debit Mastercard, where a manual signature is the principal means of verifying the authority to give the instruction;
- the Debit Mastercard Card details without the card being present at a merchant or supplier (e.g. transactions with online merchants or Recurring Payments);
- the Debit Mastercard and Contactless payments at merchant terminals; or
- the Debit Mastercard card details, or Virtual Card Card details, or inserting the Debit Mastercard into EFT terminals only; or
- the Debit Mastercard or Virtual card using a Mobile Wallet whether or not involving the use of a Biometric Identifier; to access your nominated account.

The Debit Mastercard or Virtual card cannot be used to access more than one nominated account.

All references in this Part to "nominated account" are taken to include a reference to "Nominated Account".

## 3.2 All Debit Mastercards remain our property

All Debit Mastercards remain our property at all times. You agree to return a Debit Mastercard to us:

- on request by us;
- when you close your nominated account; or
- when electronic access to your nominated account has been cancelled in accordance with clause 1.9.

## 3.3 Additional cardholder

If your nominated account permits, you may request us in writing to issue a Debit Mastercard and PIN to an additional cardholder. Each Debit Mastercard issued in relation to the nominated account will have a unique card number. The relevant provisions of these Conditions of Use apply to the additional cardholder's use of the Debit Mastercard and PIN to access your nominated account.

You are responsible for informing the additional cardholder how to use the Debit Mastercard and PIN. We suggest that you provide the additional cardholder with a copy of these Conditions of Use. A copy of these Conditions of Use can be obtained from our website (bankwest.com.au). You and not the additional cardholder will be liable for all transactions made by the additional cardholder on your nominated account using the Debit Mastercard until the additional cardholder's authority is cancelled.

An additional cardholder's authority is cancelled only when:

- we have received your request to cancel that person's Debit Mastercard; and
- that Debit Mastercard has been returned to us for cancellation, or we are satisfied, acting reasonably, either that the Debit Mastercard has been destroyed or that you have taken all reasonable steps to procure its return to us.

It is your responsibility to ensure that the additional cardholder's Debit Mastercard is returned to us. You consent to the additional cardholder having access, in respect of nominated accounts, to information about the account balance, payments, purchases and cash advances.

## 3.4 Use of the Debit Mastercard

In order to use a Debit Mastercard, you (or, if your account is in more than one name, each of you) and each other user will need to activate a Debit Mastercard upon receipt by phoning us on the number we give you for that purpose, by logging on to Bankwest Online Banking or by following any instructions we may give you.

The Debit Mastercard is valid only for the period (if any) indicated on it. The Debit Mastercard must be signed as soon as it is received.

The Debit Mastercard must be destroyed by cutting it in half diagonally and through the card details and any electronic microchip when it has expired or otherwise ceased to be valid.

If a Debit Mastercard 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.

### 3.4a Use of a Virtual Card

A single-use basis Virtual Card 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 details.

The following applies to the use of a multi-use basis Virtual Card:

- you have the choice to set an optional spend limit on funds able to be accessed;

- you must select a card end date; and

- subject to your available balance, you may make multiple transactions using the card until whichever of the following occurs first:

. any spend limit is reached (relevant only if you have set a spend limit); or

. the card end date.

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 details

If a Virtual Card 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.

## 3.5 Types of transactions that can be made using a Debit Mastercard

The following transactions can be performed by using the Debit Mastercard and PIN to access a nominated account:

- withdrawals;
- purchases;
- transfers;
- deposits;
- obtain the balance on a nominated account; and
- request a statement.

Purchases can also be performed by using the Debit Mastercard in an imprinter and signing a transaction voucher, or by giving the card details by mail order, telephone or online. Purchases of an amount up to the Contactless payment threshold can also be performed by using the Debit Mastercard and Contactless payments at merchant terminals.

Not all types of transactions apply to all nominated accounts. It may not be possible to use all EFT terminals to carry out applicable transactions on nominated accounts.

For further information call our Contact Centre.

### 3.5a Types of transaction that can be made using a Virtual Card

The following transactions can be performed by using a Virtual Card and PIN, when required, to access a nominated account:

– purchases;

– withdrawals at selected merchants

## 3.6 Where the Debit Mastercard and Virtual Card, and PIN can be used

Users can use the Debit Mastercard and PIN:

- at any ATM or EFTPOS terminal in Australia;
- at selected agents;
- by selecting the Credit, Cheque or Savings key on the keyboard. If the Cheque or Savings key is selected, our Electronic Withdrawal Fee may apply. Refer to the relevant Product Schedule message us in the Bankwest App or contact our Contact Centre for details of this fee.

Users can also use the Debit Mastercard and PIN at any ATM overseas which displays the Mastercard symbol, only by selecting the Credit key on the keyboard. Users may be able to use the Debit Mastercard and Contactless payments at an overseas merchant terminal in some cases for transactions equivalent to the Contactless payment threshold.

Users can use the Virtual Card and PIN at any EFTPOS terminal in Australia;

A Virtual Card cannot be used at an ATM.

## 3.7 Where the Debit Mastercard and Virtual Card can be used without a PIN

Users can use the Debit Mastercard without a PIN:

- in Australia, depending on the Card;
- over the counter at financial institutions and merchants; and
- overseas at ATMs and merchant terminals which display the Mastercard symbol.

Users can use the Virtual Card without a PIN:

- in Australia;
- over the counter at merchants; and
- overseas at merchant terminals which display the Mastercard symbol.

If a merchant accepts payment with your Debit Mastercard or Virtual 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 the Debit Mastercard and the Virtual card.

## 3.7a Where the Debit Mastercard and Contactless payments can be used

Users with the Debit Mastercard with the EMVCo Contactless Indicator on the front of the card can perform Contactless payments transaction.

To make a purchase using Contactless, 'tap' your Debit Mastercard on the merchant terminal and wait for the transaction confirmation. You should make sure the correct transaction details are displayed on the merchant terminal and you should not generally need to hand your card over to the merchant, sign or enter a PIN to complete the transaction.

You can also use your Debit Mastercard with Contactless payments anywhere EMVCo Contactless Indicator is displayed. You can still enter a PIN at EFT terminals or provide a signature in some cases depending on your Card, even if your card is enabled with Contactless payments.

## 3.7b Where the Debit Mastercard and Virtual Card can be used with a Mobile Wallet

A Debit Mastercard or Virtual Card may be used with a Mobile Wallet we approve for use from time to time to make payments to retailers and payments within Mobile Wallet applications. A Mobile Wallet provider may impose age (or other) restrictions on using a Debit Mastercard or Virtual Card in a Mobile Wallet.

If the dollar value of a transaction initiated using a Mobile Wallet exceeds any payment threshold applying to a Debit Mastercard or Virtual Card, a user may need to enter the PIN associated with the Debit Mastercard or Virtual Card, to initiate the 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 terminal will allow the user to initiate a 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 Debit

Mastercard, or Virtual Card (as relevant) selected as the default card within the Mobile Wallet in order to use the Debit Mastercard or Virtual Card when making a 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 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 Debit Mastercard or Virtual Card loaded to a Mobile Wallet:**

Before we can allow a Debit Mastercard or Virtual Card to be added to a Mobile Wallet:

- we must verify the user's identity; and
- the Debit Mastercard must not be closed, reported lost or stolen or its balance written off.

A Debit Mastercard Card of an additional cardholder cannot be deleted or cancelled in a Mobile Wallet, however, you may suspend or cancel an additional cardholder's Debit Mastercard by contacting Bankwest at anytime on 13 17 19 or by messaging in the Bankwest App. It may be possible to make 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 Debit Mastercard or Virtual Card with a Mobile Wallet, the Debit Mastercard or Virtual Card should be removed from the Mobile Wallet prior to deleting or uninstalling it on the mobile device. Other ways to ensure that a Debit Mastercard or Virtual 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 Debit Mastercard or Virtual 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 Debit Mastercard or Virtual Card may also be removed from a Mobile Wallet by the Mobile Wallet provider 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. 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 Debit Mastercard or Virtual 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;

– we suspect on reasonable grounds that your account is being used in a way that results in or may cause financial abuse.

– 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 Account Access Conditions of Use or the terms and conditions specific to the account.

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

## 3.8 Daily transaction limits

a) At ATMs

The minimum amount users can use a Debit Mastercard to withdraw each day from CommBank ATMs is $20 or $50 (depending on the ATM).

A maximum daily transaction limit also applies. Users will be advised of this limit when their Debit Mastercard is issued.

The minimum and maximum cash withdrawal limits applying to non-CommBank ATMs may vary.

A Virtual Card cannot be used to withdraw cash at any ATM.

b) Our agents and EFTPOS terminals

The maximum aggregate amount that can be withdrawn daily from our agents that provide withdrawal services and when making purchases from EFTPOS merchants using a Debit Mastercard and PIN is the maximum daily transaction limit.

Merchants, our agents, non-Bankwest-branded outlets, and other financial institutions may have additional restrictions on the amount of funds that may be withdrawn, paid or transferred.

A Virtual Card cannot be used to withdraw cash (or make transfers) at our agents. However, a Virtual Card may be used to withdraw cash from selected merchants. The cash withdrawal limit at a merchant is the lower of any spend limit applying to the Virtual Card and any cash withdrawal limit determined by Mastercard and the merchant's bank.

## 3.9 Depositing funds using the Debit Mastercard and PIN

You can deposit funds to your nominated account at selected agents and select CommBank ATMs. There are limits on the amount of cash you can deposit at our agents and at ATMs (see the Bankwest website for details). If a cheque (not being a foreign cheque, in any currency) is deposited to the account, the amount of the cheque will be credited on the business day it is received by us but it will not be available to you until it is cleared. All deposits made at CommBank ATMs are checked by us. If the amount appearing on the transaction record differs from the amount actually received by us, we will credit your nominated account with the amount actually received and notify you as soon as possible.

We accept responsibility for the security of deposits received at CommBank ATMs subject to checking of the amount deposited. The amount checked by us is evidence of the amount actually received unless the contrary is established.

There is no facility for payments to be made to nominated accounts using the Debit Mastercard and PIN whilst overseas. If you wish to make automatic payments or payments in advance contact our Contact Centre or message us in the Bankwest App.

A Virtual Card cannot be used to deposit funds anywhere – including at agents or at ATMs.

## 3.10 Transactions needing authorisation

Transactions on nominated accounts may need to be authorised by us. We may decline to authorise a transaction if:

- you are behind in making payments to a nominated account;
- the credit limit on a nominated account would be exceeded;
- there are insufficient funds in a cheque or savings nominated account; 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.

## 3.11 Transactions at EFT Terminals

When a user makes an EFT transaction at an EFT terminal using the Debit Mastercard and PIN, Debit Mastercard and Contactless payment, or Virtual Card (either with or without a PIN) 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 nominated accounts on the day they are made. Processing may take a number of days. We will process transactions to your nominated accounts 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.

## 3.12 Use of a Debit Mastercard or Virtual Card 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 or a financial institution who:

- refuses to honour a Debit Mastercard or Virtual Card; or
- imposes limits or conditions on use of a Debit Mastercard or Virtual Card.

Debit Mastercard or Virtual Card promotional material and material promoting EFTPOS or Mastercard displayed on premises of merchants, financial institutions and our agents is not a warranty by us that EFTPOS or Mastercard facilities are available or that goods and services may be purchased using the Debit Mastercard or Virtual Card.

Unless required by law we will not be liable for goods or services supplied using a Debit Mastercard or Virtual Card. 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 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 you later decide not to take the goods or use the services;

you authorise the merchant to complete the transaction.

## 3.13 When we may block or decline a transaction

You may only use your Debit Mastercard, Virtual Card or payment device for lawful purposes.

In addition to our rights under clause 1.9(a) (“Cancellation of 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 4

# Phone Banking and Bankwest Online Banking Conditions of Use

## 4.1 About these conditions

Part 4 (together with Parts 1, 7, 8, 11 and 12) of these Conditions of Use applies to all transactions involving the use of Phone Banking* and Bankwest Online Banking* to access your nominated accounts.

* Including the BPAY scheme

## 4.2 What is Phone Banking?

Phone Banking is a service provided by us which enables a user to make enquiries and effect transactions on nominated accounts 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.

## 4.3 What can you do using our Phone Banking services?

Users can:

- obtain the balance of a nominated account;
- transfer funds between nominated accounts;
- make bill payments electronically through BPAY (excluding Osko Payments);
- postdate funds transfers and bill payments up to
- 90 days in advance;
- make payments to a nominated credit card account;
- enquire on transactions on a nominated account;
- order a statement on a nominated account;
- order a statement of interest for taxation purposes; and
- change a password.

## 4.4 How to use our Phone Banking services

To be able to use Phone Banking a user must have received a PAN and password from us.

We will advise the PAN and password separately.
To use Phone Banking users must:

a) Call Phone Banking on 13 17 18 for the cost of a local call Australia wide; (calls from mobile phones and calls made from overseas are charged at the applicable rate);

b) enter their PAN using the telephone key pad;

c) enter their password using the telephone keypad; and

d) follow the instructions given.

## 4.5 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 approved internet browser software, and a mobile device using the Bankwest App, which enables a user to make enquiries and effect transactions over the Internet on nominated accounts using a PAN and password.

Bankwest will begin to make the new Bankwest App available to select customers from 25 February 2025.

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.

## 4.6 What can be done using our Bankwest Online Banking services?

Users can:

- obtain the balance of a nominated account;
- transfer funds between nominated accounts;
- make bill payments electronically through BPAY;
- make payments using Pay AnyBody;
- register and manage a PayID and Payment Agreements;
- enquire on transactions on a nominated account;
- perform a range of administrative functions;
- (for some products), make international transfers in overseas currency ; and
- manage communication preferences (including push notifications which we may send from time to time).

Bankwest may, in accordance with our Privacy Statement, if you have registered for the App on a device, send you push notifications (if enabled on your device) and in-app messages including important service-related messages, commercial electronic messages and direct marketing about products and services that may be of interest to you. You can opt out of receiving such messages at any time by calling 13 17 19, by using the unsubscribe function for commercial electronic messages or by changing your notification preferences in your settings.

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 4.6 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.

## 4.7 How to use our Bankwest Online Banking service

To access Bankwest Online Banking, a user must have a PAN and a password.

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

Users without a security token logging on to Bankwest Online Banking for the first time or any other time we require 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 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 4.6.

## 4.8 Internet security and privacy

Users of Bankwest Online Banking should take all reasonable steps to protect the security of their computer hardware and software, and mobile device. For instance, users should ensure their computer and mobile device is free of viruses and should not leave their computer or mobile device unattended while logged on to Bankwest Online Banking. These steps will not determine your liability for unauthorised transactions. Liability for unauthorised transactions will be determined in accordance with Part 8 of these Conditions of Use and the ePayments Code.

## 4.9 Access & Restrictions of access to services

Access to our Phone Banking and/or Bankwest Online Banking services may not be available from some States, Territories or Western Australia 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 our Phone Banking and Bankwest Online Banking services on a 24 hour continuous basis. However, circumstances may not always make this possible, such as the quality of telephone lines, the type of telephone or telephone exchange.

If our Phone Banking and/or our Bankwest Online Banking service cannot be accessed at any time, please advise our Contact Centre to enable us to investigate the reason.

Should Phone Banking or Bankwest Online Banking not be available users should ensure they have adequate contingency plans in place to effect transactions and obtain account information. Subject to clause 8.7 (When the electronic banking system or EFT terminal breaks down), 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.

Transactions (except BPAY, Pay Anybody and international transfers) which are made on a business day up to 6.00pm WST should be processed that day. Transactions (except BPAY, Pay Anybody and international transfers) which you make on a non-business day or after 6.00pm WST on a business day 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.

### 4.9a 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:

- refuse to process or complete any transaction or dealing of yours; and/or
- 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.

## 4.10 Nominated accounts

You may nominate a maximum of 12 accounts per PAN as nominated accounts.

You must be authorised to operate each nominated account alone (i.e. own account, or joint account which you are authorised to operate alone).

## 4.11 BPAY payments

This clause does not apply to Faster Payments (including Osko Payments).

a) If there is any inconsistency between the provisions of clause 4.11 and the Account Access Conditions of Use, clause 4.11 prevails to the extent of that inconsistency.

b) All bill payments that are made through our Phone Banking and Bankwest Online Banking 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).

c) When you tell us to make a BPAY payment, you must give us the information specified in paragraph (e) below. We will then debit your nominated account with the amount of that BPAY payment.

d) 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 in Bankwest Online Banking or by 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.

c) 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 nominated account to be debited for the payment.

f) We shall not be obliged to effect a BPAY instruction if the information is incomplete and/or inaccurate, there are insufficient cleared funds in the account to be debited, or the BPAY payment will cause you to exceed your daily BPAY payment limit.

g) If there is any inconsistency between the Conditions of Use applying to the nominated account to be debited and these BPAY Conditions of Use, the BPAY Conditions of Use will apply to the extent of that inconsistency.

h) Except for postdated payments (clause 4.11(n)) we will not accept an order to stop a BPAY payment once we have been instructed to make the BPAY payment.

i) Our payment cut-off time for a BPAY payment is 4.00pm WST.

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

   - on the date we are told to make that BPAY payment, if we receive the instruction before our payment cutoff time on a business day; or
   - on the next business day, if we receive the instruction after our payment cut-off time on a business day, or on a non-business day.

k) A delay may occur in processing a BPAY payment where:

- there is a public or bank holiday on the day after we are told to make a BPAY payment; or
- a biller, or another financial institution participating in the BPAY scheme, does not comply with its obligations under the BPAY scheme.
- While it is expected that any such delay will not continue for more than one business day, it may continue for a longer period.

l) Users must be careful to tell us the correct amount to be paid to a biller. If the amount we were instructed to pay was greater than the amount you intended to pay, you must contact the biller to obtain a refund of the excess. If the amount we were instructed to pay was less than the amount needed to be paid, another BPAY payment should be made for the difference between the amount actually paid to a biller and the amount needed to be paid.

m) If we are advised that a BPAY payment cannot be processed by a biller, we will:

i) advise you of this;

ii) credit your account with the amount of the BPAY payment; and

iii) take all reasonable steps to assist in making the BPAY payment as quickly as possible.

n) Postdated BPAY payments

i) A BPAY payment may be requested for a date in the future, however, we will only make the BPAY payment if sufficient cleared funds are available in the nominated account from which the BPAY payment is to be made by 11:30pm WST on the business day prior to the scheduled BPAY payment date and the BPAY payment will not cause you to exceed your daily BPAY payment limit on the date stipulated for the payment to be made.

If the date stipulated is not a business day, or is a non-existent day (for example, a BPAY payment is scheduled for the 31st of each month in months where there are only 28, 29 or 30 days), we will make the BPAY payment on the next business day. In the event that there are insufficient cleared funds or your daily BPAY limit 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.

o) We may charge a fee to correct errors on your nominated accounts due to incorrect BPAY instructions.

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

q) You should check your nominated accounts carefully and promptly report to us, as soon as you become aware of them, any BPAY payments that you think are errors or are BPAY payments that you did not authorise. (Note: The longer the delay between the date of your BPAY payment and when you tell us of the error, the more difficult it may be to correct the error.

For example, we or your biller may not have sufficient records or information available to us to investigate the error. If this is the case, you may need to demonstrate that an error has occurred, based on your own records, or liaise directly with the biller to correct the error.)

r) Your liability for unauthorised and fraudulent BPAY payments will be determined in accordance with Part 8.

s) Liability for mistaken payments

If a BPAY payment is made to a person or for an amount, which is not in accordance with the instructions (if any) given to us and your account was debited for the amount of that payment, we will credit that amount to your account. However, if you are responsible for a mistake resulting in that payment and we cannot recover the amount from the person who received it within 20 business days of us attempting to do so, you must pay us that amount.

t) Biller consent

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

u) Consequential damage and indemnity

Subject to Part 8 of the 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 our negligence or that of our 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 these BPAY Conditions of Use.

## 4.12 International Transfers

If there is any inconsistency between the provisions of clause 4.12 and the remainder of the Account Access Conditions of Use, clause 4.12 prevails to the extent of that inconsistency.

When you tell us to make an international transfer, you:

i) must give us the information specified in this clause 4.12 or that we otherwise request;

ii) confirm that all details you have provided in connection with the transfer are true and correct; and

iii) authorise us to debit the account that the payment is being made from with the total payment and the fees and charges specified in these terms and conditions.

For Bankwest Online Banking, the initial maximum aggregate amount of international transfers you may instruct us to make on any business day is zero.

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 in Bankwest Online Banking or by calling our Contact Centre 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.

For Online Business Banking, the Daily Payment Limit applies. You can instruct us to make multiple International transfers on any business day up to your Daily Payment Limit. However, the initial monetary limit for each International transfer Instruction you can ask us to make on any business day is the equivalent of $100,000.00 AUD, unless your Daily Payment Limit is lower than $100,000.00 AUD, in which case that lower limit will apply. Each International transfer will incur a fee. Different limits may apply for Online Business Banking transactions requested using devices referred to in clause 3.1. of the Bankwest Online Business Banking Product Disclosure Statement. To arrange a different Daily Payment Limit or for more information, please contact the Business Customer Support Team on 13 7000.

In the absence of any arrangements between you and Bankwest, you can only give an Instruction for an international transfer up to the available balance of your selected nominated account. The aggregation of any available balances of other nominated accounts is not possible in determining the available balance for the selected nominated account. If an international transfer made in accordance with an Instruction overdraws a nominated account you must immediately repay the amount overdrawn.

The following information must be given to us to make an international transfer and foreign exchange transaction:

i) The destination country for your payment;

ii) The account details of the account that you want to make the payment from – BSB, account number;

iii) The account details of the account that you want to make the payment to – recipient's full name, residential address, BSB/sort code/ABA or routing number/bank or branch code, swift code/BIC code, account number;

iv) For international transfers – currency and amount, reason for transfer and statement messages.

We shall not be obliged to effect a payment instruction if the information is incomplete and/or inaccurate, there are insufficient cleared funds in the account to be debited, there is a technical failure which prevents us from processing the international transfer, a hold has been placed on the account from which the international transfer is to be sourced, the payment will cause you to exceed your daily international transfer payment limit, or in the case of Online Business Banking, a qualified Master User has not authorised the international transfer.

Once an international transfer Instruction has been given, it may not be possible to recall the international transfer or prevent it from being made.

If you want to amend or recall a payment you have requested, please contact Contact Centre or the Business Customer Support Team. However, if we have already processed your payment request, the payment cannot be recalled unless the law of the destination country permits this and the beneficiary first authorises their financial institution to facilitate the recall.

Bankwest will accept the return of your payment if the payment is refused for any reason. A returned payment will be credited to the account to which the payment was originally debited (unless you instruct Bankwest to credit another Bankwest account you hold that is in the same currency of the originally debited account). If a returned payment requires a currency conversion, Bankwest will convert the returned payment to the currency of the originally debited account using Bankwest's applicable foreign exchange rate on the day the returned payment is credited to your account.

Please note Bankwest fees and beneficiary Bank fees will apply to make amendments, send a trace or to recall a payment whether or not we are able to amend, trace, recall, prevent or recover the international transfer.

To the extent permitted by law, we will not be liable for any loss or damage (including loss or damage arising due to variations in foreign exchange rates) directly or indirectly resulting from:

i) delays in Bankwest or any other institution making the payment;

ii) any act or omission of any other institution;

iii) Bankwest acting on these instructions; or

iv) any losses or damage as a result of a returned payment.

Bankwest's maximum liability to you in relation to an International transfer, including for any negligent act or omission of Bankwest, is the Australian dollar amount of the international transfer. In calculating the Australian dollar amount, we will use our currency conversion rates which we applied on the date on which we processed your international transfer instruction.

We may use other financial institutions to make the payment to the beneficiary. We may receive a commission from the other institutions.

We will complete a currency conversion prior to sending your payment in overseas currency. The receiving beneficiary financial institution and any intermediary institution, may also complete a currency conversion.

The conversion of the funds to a local or other currency at their country of destination is subject to the banking systems of the countries or other institutions through which the payment is made and is therefore beyond our control.

Where the beneficiary account overseas is held in Australian currency, you agree that the beneficiary financial institution may re-convert to AUD at the prevailing currency exchange rate at the time of receipt. If that happens, the beneficiary may receive less than the amount that you requested us originally to send.

The time taken for a payment to reach the beneficiary account depends on the banking systems of the countries or other institutions through which the payment is made and it depends on the provision of correct and complete beneficiary information.

A payment sent overseas to a major financial centre or to a destination in North America, the United Kingdom or Western Europe will normally be received by the beneficiary within one week. Other overseas destinations may take much longer, and this timing is beyond our control.

Other institutions (including intermediary banks and the beneficiary's bank) may charge a fee for handling the international transfer or for making the payment to the beneficiary. If other institutions charge a fee, they will deduct their fee from the payment (so the beneficiary will receive a lesser amount than your original request to us to remit). The amount of any fees imposed by other institutions is beyond our control and subject to the rates set by those other institutions (which may vary between countries).

However, where an international transfer is made in foreign currency, we will absorb fees imposed by other institutions for handling the international transfer – with the exception of fees (if any) charged directly to the beneficiary's account by the beneficiary's financial institution.

Where an International Transfer is made in AUD, Bankwest will not absorb fees imposed by other financial institutions involved in the transfer (Note – Bankwest cannot provide an estimate of the amount of such fees.) Additionally, fees may also be charged directly to the overseas account by the beneficiary's financial institution.

The payment will be made to the beneficiary account number you provide in Bankwest Online Banking or Online Business Banking. The receiving institution may not check that the beneficiary's name you provide matches the beneficiary account number you provide.

It is therefore essential that you check that the beneficiary account number you provide is correct and is in the correct format. Neither Bankwest nor any other institution is liable for any loss resulting from errors in the beneficiary account number you provide or the beneficiary account number being provided in the incorrect format. You acknowledge that overseas financial institutions may not have the same protocols as Australian financial institutions for resolving mistaken payments, meaning that if you make a mistake inputting account details, there is a higher risk that the mistaken payment may not be recovered.

If beneficiary details are provided in an incorrect format, this may cause an overseas financial institution to credit the international transfer to an account you do not intend.

We may delay, block, freeze or refuse to make a payment where we have reasonable grounds to believe that making the payment may breach Australian law or the law of any other country. You will provide any additional information we reasonably require to comply with Australian law or the law of any other country. In order to make this payment, personal information relating to individuals named in this form may be processed for the purposes of:

i) complying with applicable laws, including without limitation anti-money laundering and anti-terrorism laws and regulations; and

ii) fighting crime and terrorism, including disclosure to any government entity, regulatory authority or to any other person we reasonably think necessary for those purposes. This may mean that personal information will be transferred overseas to countries that are not subject to privacy obligations equivalent to those which apply within Australia. You agree to the processing and transfer of your personal information relating to any other individuals that you provide.

To the extent permitted by relevant legislation you agree to keep Bankwest indemnified against any claims that may be made against Bankwest by reason of us having acted on your instruction to make an International transfer.

## 4.13 Limits

At our discretion we may impose and/or vary minimum and/or maximum limits on the amounts which you may transfer or you agree to be transferred, as relevant, from your nominated accounts using our Phone Banking and/or Bankwest Online Banking services or under a Payment Agreement. Without limiting the above, circumstances where we may reduce or remove these limits include:

– where you have requested a higher payment limit and have not made a transaction utilising any of that increased limit within the last month ; or

– we believe it is reasonably necessary to protect you or us from possible fraudulent activity, scams or other activity that might cause you or us to lose money.

When we do this we will act fairly and reasonably towards you. We will not be responsible for any loss or damage, cost, expense or other inconvenience you incur except to the extent that we act negligently in taking any action under this clause.

We may also impose limits on the value of Payment Agreements we allow you to authorise each day.

Current information on these limits, including any changes to them, can be accessed in Bankwest Online Banking or by messaging us in the Bankwest App.

## 4.14 Other matters

We shall issue a receipt number for each funds transfer or BPAY payment instruction received via Phone Banking or Bankwest Online Banking. When we have instructions for more than one transfer or BPAY payment from a nominated account we may determine the order of priority in which the transfers or payments are made. In making any such determination, we will act reasonably. You must ensure that your account from which a transfer or BPAY payment is to be made has sufficient available funds to enable the transaction to be performed by us.

If a funds transfer or BPAY payment is scheduled for a future stipulated date, it will only be effected on that date by us if sufficient cleared funds are available in your nominated account (for non-Faster Payments, such funds must be available by 11.30pm WST on the business day prior to the scheduled transfer date), and the funds transfer or BPAY payment will not cause you to exceed any limit we impose or your daily BPAY payment limit, as relevant.

We do not guarantee to give effect to any payment instruction received via Phone Banking or Bankwest Online Banking. We may delay and/or refuse to give effect to any Phone Banking or Bankwest Online Banking instruction without notifying you. Circumstances where instructions will not be processed include:

- when the Conditions of Use of the nominated account prohibit the payment(s);
- when the nominated account has insufficient available funds to cover the intended payment(s);
- when the BPAY payment will cause you to exceed your daily BPAY payment limit; or
- when the payment would cause you to exceed any transaction limit applying to payments.

## 4.15 Authorised Users

If you (whether an individual, company, partnership or unincorporated association) have authorised a signatory to operate a nominated account, that signatory may, if you request it and we agree, have Phone Banking and/or Bankwest Online Banking access to that nominated account with that person's own PAN and password.

The relevant provisions of these Conditions of Use apply to the authorised user's access to the nominated account and you will be liable for all transactions made by the authorised user until that user's authority is cancelled.

Part 5

# Pay AnyBody Conditions of Use

## 5.1 About these conditions

Part 5 (together with Parts 1, 4, 7, 8 and 11) of these Conditions of Use applies to all transactions involving the use of the Bankwest Online Banking Pay

AnyBody Service (Pay AnyBody). The Pay AnyBody

Conditions of Use operate in conjunction with the

Conditions of Use applicable to Bankwest Online Banking (see Part 4 above) and to your nominated accounts accessed using these services. The Pay AnyBody Conditions of Use prevail to the extent of any inconsistency.

Note: a payment made under the PayTo Service is not a Pay AnyBody payment. Instead, PayTo Service payments are addressed in Part 12. References in this Part 5 to Faster Payments do not include payments made under the PayTo Service.

## 5.2 What is Pay AnyBody?

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

a) another person's account held with us; or

b) another person's account or another account held by you with the Commonwealth Bank of Australia or another financial institution (except non- Bankwest-branded credit card accounts), by either:

   i) using the BSB number, account number and account name for the other person's account; or

   ii) making an Faster Payment either through using:

a) the PayID of the other person; or

b) the other person's BSB number, account number and account name.

Note – a payment made under the PayTo Service is not a Pay AnyBody payment. Instead, such payments are governed by Part 12.

## 5.3 Daily Pay AnyBody payment 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 limits 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 or by 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.

## 5.4 Making a Pay AnyBody payment

The following information must be given to us to make a Pay AnyBody transfer:

i) in respect of the account to which the funds are to be transferred:

   Either

   – the BSB number;

   – the account number; and

   – the account name; or

   – (when we advise you of the availability of this functionality), the recipient's PayID; and

ii) a description of the transaction (except for Faster Payments).

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 prompt 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, there are insufficient cleared funds in the account from which the debit is to be made, or the transfer will cause you to exceed your daily Pay AnyBody payment limit or any limits applying to Faster Payments.

If we permit a User to make a Faster Payment from a credit card account, no "chargeback" rights will be available in relation to the Faster Payment.

## 5.5 Postdated Pay AnyBody transfers

This clause applies to all Pay Anybody transfers except Faster Payments. However, when we advise you of the availability of this functionality for Faster Payments, this clause will also apply to Faster Payments.

a) A Pay AnyBody transfer may be requested for a date up to three years into the future, however, we will only make the Pay AnyBody transfer if sufficient cleared funds are available in the nominated account from which the transfer is to be made by 11.30pm WST on the business day prior to the scheduled Pay AnyBody transfer date and the transfer will not cause you to exceed your daily Pay AnyBody payment limit on the date stipulated for the transfer to be made. If the date stipulated is not a business day, or is a non-existent day (for example, a transfer is scheduled for the 31st of each month in months where there are only 28, 29 or 30 days), we will make the Pay AnyBody transfer on the next business day. This will result in this amount not being included in the account balance for the receiving account until the transfer is complete (eg next business day or later). In certain circumstances this may impact qualifying for possible benefits on the receiving account. For example, if a Pay AnyBody transfer is scheduled from a Bankwest account into your Hero Saver account, and this is to occur on the last day of the month which happens to fall on a non-business day, you will not meet the criteria for bonus interest for that month (if sufficient payments into the Hero Saver account for that month have not otherwise been made). In that scenario, the funds transferred into the Hero Saver account will count towards qualifying for the bonus interest for the following month.

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.

## 5.6 Cancelling a Pay AnyBody transfer

A Faster Payment cannot be cancelled once it has been processed. For non-Faster Payments, it may be possible in some cases to cancel an initiated Pay Anybody transfer. However, we are not obliged to cancel a Pay AnyBody transfer once we have accepted the instruction to make it. If we cancel a Pay Anybody transfer, a fee may be payable for any such cancellation.

## 5.7 Processing Pay AnyBody transfers

Note: Paragraphs (a) and (b) apply only to Pay AnyBody transfers which are not Faster Payments. Paragraph (c) and (d) apply to all Pay Anybody transfers (including Faster Payments).

a) Our payment cut-off time for a Pay AnyBody transfer to be effected to another Bankwest branded account on the same day is 3.00pm WST.

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

   – on the date we are told to make that Pay AnyBody transfer, if we receive the instruction before 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.

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

- we need to verify that the transaction is an authorised transaction;
- there is a public holiday on the day or the day we are told to make a Pay AnyBody transfer;
- another financial institution participating in the Pay AnyBody transfer scheme does not comply with its obligations under that scheme;
- the transfer is a First Time Payment; or
- we exercise our discretion under these Conditions of Use to delay the processing of the transfer.

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

- advise you of this;
- credit your 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.

## 5.8 Liability for unauthorised transactions and fraud

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

## 5.9 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 (if any) given to us, and your account was debited for the amount of that payment, we will credit that amount to your account.

## 5.10 Mistakes as to the amount of a Pay AnyBody transfer

Users must be careful to tell us the correct amount to be transferred. If the amount we were instructed to transfer was greater than the amount intended you must contact the other person or their financial institution to obtain a refund of the excess. If the amount we were instructed to transfer was less than the amount needed to be paid another Pay AnyBody transfer should be made for the difference between the amount actually paid and the amount intended to be paid.

## 5.11 PayID and Faster Payments

PayID is a Faster Payment addressing service that enables a payer to make a Faster Payment to a payee using an alternative identifier instead of a BSB and account number.

A PayID can also be nominated in a Payment Agreement and used for the purpose of debiting an account under that Payment Agreement (see Part 12).

## 5.12 Participation in PayID

Participation in the PayID service is optional and Bankwest will not register a PayID for you without your consent. You consent to participation in the PayID service when you complete the PayID registration process. We will provide you with the terms and conditions applying to participation in the PayID service during the PayID registration process. After we advise you of the availability of the PayID registration process, you can register a PayID via Bankwest Online Banking. We may require you to use a single-use code (or similar) that we send to you for the purpose of registering a PayID.

## 5.13 Making Faster Payments

After we advise you of the availability of each of these functions, a User may use Bankwest Online Banking to make a Faster Payment to:

a) a payee's PayID; or

b) a payee's BSB and account number, provided that:

c) we and the payee's financial institution support the particular Faster Payment service;

d) the payee's account is eligible to receive the particular Faster Payment;

e) the Faster Payment would not exceed any transaction limits applying to Faster Payments; and

f) for a Faster Payment to a PayID), the PayID is not locked.

A User must check that a payee's PayID name that is displayed matches the person the User intends to pay. If it does not match the intended payee's name, then the User must contact the intended payee to confirm that all details are correct before proceeding to make the Faster Payment.

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. We may use our NameCheck technology 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 NameCheck prompt 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. NameCheck prompts are based on our available payment information, but we are not able to confirm that the name actually matches the account.

We may restrict the ability of a User to make a Faster Payment (whether to a PayID or to a BSB and account number) to a particular version or channel of Bankwest Online Banking - such as via the Bankwest App.

## 5.14 Receiving Faster Payments to a PayID

Before you can receive a Faster Payment to your PayID, you must register your PayID.

## 5.15 Payment errors

We will ensure that your PayID and nominated details are accurately recorded in the PayID service. Where we and the sending financial institution determine that a Faster Payment made to your nominated account is either a mistaken internet payment (made by the sender of the Faster Payment) or a Misdirected Payment, we may, without your consent, and subject to complying with any other applicable terms and conditions, deduct from your nominated account an amount equal to that payment. We will notify you if this occurs.

## 5.16 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. We have also adopted those processes for all Faster Payments. They do not apply to:

   i) transactions (including Error Payments) where the Pay Anybody service used is a service designed primarily for use by a business and established primarily for business purposes; or

   ii) Faster Payment Over Payments, Faster Payments Repeated in Error or Misdirected Payments. If those errors have occurred, please contact the Bank as soon as possible.

These processes (which we agree to follow) are set out below. Subject to your rights at law and to the extent not caused by our negligence, fraud or wilful misconduct or that of our agents, 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 5.16(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 CommBank-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 CommBank-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 5.16(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 5.16(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 11 regarding how to lodge a complaint and how we will handle that complaint.

c) You may report a Mistaken Internet Payment by:

- messaging us in the Bankwest App;
- 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);
- logging on to our website (bankwest.com.au) and following the procedures it sets out for reporting a Mistaken Internet Payment; or
- writing to us at the address shown on the nominated account statement containing the suspected error.

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 ten business days.

d) This sub-clause 5.16(d) applies if we have determined that a Mistaken Internet Payment has been made to a Bankwest or CommBank-branded Eligible Recipient Account.

v) Despite paragraphs 5.16(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*.

vi) 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 CommBank, 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 5.16(d)(iii) below. If we (or CommBank, as relevant) choose to retrieve the full value of the funds from the unintended recipient account, we (or CommBank, as relevant) will use reasonable endeavours to do so.

vii) 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 ten business days after the payment is made, we will return the funds to you. We will do this within five 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 ten business days.
- If you have reported the Mistaken Internet Payment between ten business days and seven months after the payment is made, we will give the unintended recipient ten 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 two business days after the expiry of that period.
- If you have reported the Mistaken Internet Payment more than seven 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 CommBank-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 five business days and let us know whether there are sufficient credit funds in the unintended recipient's account to cover the payment.

ii) Despite paragraphs 5.16(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 of Department of Veterans' Affair 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 5.16(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 ten 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 five 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 ten business days and seven months after the payment is made, the Receiving ADI has ten 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 ten 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 two business days after the expiry of that period.

  – If you have reported the Mistaken Internet Payment more than seven 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 6

# Recurring Payments

## 6.1 About this part

This section provides you with information about Recurring Payments.

## 6.2 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.

## 6.3 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.

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.
- a Virtual 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 also 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.
- a Virtual 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 7

# Security of Access Methods

Users must protect relevant access methods to prevent unauthorised access to nominated accounts. 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.

## 7.1 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 any losses resulting from any unauthorised transactions. Liability for unauthorised transactions will be determined in accordance with Part 8 of these Conditions of Use and the ePayments Code.

Never log-in to Bankwest Online Banking from a hyperlink contained in an email, SMS, or other form of electronic communication (such as social media), or from a third party website.

**To protect the card**

- Sign the physical card as soon as it is received.
- Carry the physical card whenever possible.
- Always keep the physical 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 the card details.
- When the transaction is complete remember to take the physical card and transaction receipt.

**To protect the card details**

- Do not give or tell the card details to anyone.
- Use care to prevent anyone seeing the card details when entering them into 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 which has an easily retrievable combination (such as repeated numbers of 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 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 record.
- Do not keep different access methods together,
- for example in a bag or wallet, in a car or in the same piece of furniture.
- Do not keep a record of a secret code with any document containing the reference numbers for nominated accounts or with other account information such as statements or cheque books.
- Be ready to make the transaction when at electronic equipment.
- Be careful to prevent anyone else from seeing the secret code being entered at electronic equipment.
- Watch out for mirrors, security cameras or any means which enable other people to see the secret code being entered.
- Do not access Phone Banking or the Bankwest Online Banking website directly from a facility where the details you enter may be recorded by a third party, e.g. from a hotel telephone or a computer at an internet cafe.
- 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 the card or security token.
– Reversing the sequence of the secret code.
– 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, or disguising the secret code in any other easily understood code.
– Recording the secret code as a series of numbers or letters with any of them marked to indicate the secret code.
– You must not use any other forms of disguise which are similarly unsuitable because another person can easily work out the secret code.

**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, PANs or secret code details on the security token.
– Do not drop the security token or expose it to high heat, water or attempt to disassemble 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 device and 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 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.

**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.

**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, attempt to disassemble 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.

**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;
- you or any user suspects that someone has used the mobile device or a secret code to conduct a transaction or otherwise tried to access the mobile device or Mobile Wallet.

## 7.2 Reporting loss, theft or unauthorised use of a card, security token, Payment Device or breach of security of a secret code

If:

- a card;
- Payment Device;
- security token; or
- mobile device on which a card has been loaded using a Mobile Wallet, is lost, stolen or used without authorisation or a secret code becomes known to someone else, you or any additional cardholder or authorised user must immediately tell us by telephoning our Contact Centre on the following number: **13 17 19** (24 hours).

If you are overseas, telephone 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). When we are told, we will acknowledge receipt of the notification by giving the user a notification number. This should be kept as proof of the date and time of the report. If for any reason the Contact Centre telephone hotline is unavailable and this prevents notification, you will not be liable for any unauthorised transaction which could have been prevented during this period if the telephone facility had been available, provided we are notified within a reasonable time of the Contact Centre telephone hotline becoming available again.

If you have a Debit Mastercard or Virtual Card, instead of telling us, you or (where relevant) any additional cardholder can alternatively tell any bank displaying the Mastercard symbol that a card is lost, stolen or used without authorisation, or that a secret code has become known to someone else.

Part 8

# Liability for Unauthorised Transactions and for system or equipment malfunctions

## 8.1 Application of this Part

This Part deals with liability for transactions which are carried out without the knowledge and consent of a user except where a Mobile Wallet is used. It also deals with liability where the electronic banking system or an EFT terminal malfunctions. Part 9 deals with liability for transactions made using a Mobile Wallet.

## 8.2 Authorised transactions

You are liable for all transactions carried out in respect of your nominated accounts 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.

## 8.3 When you are not liable for EFT transactions

You will not be liable for losses in respect of a nominated account caused by an unauthorised EFT transaction:

a) resulting from unauthorised use of a card, security token, Payment Device or secret code which forms part of an access method, before the user has received the card, Payment Device, security token or secret code (as relevant);

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

c) relating to any component of an access method that is forged, faulty, expired or cancelled;

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

   – us;

   – any organisation involved in the provision of the EFT system; or

   – any merchant;

e) where it is clear that the user has not contributed to the loss; or

f) caused by the same transaction being incorrectly debited more than once to the same account.

Please note that a Mistaken Internet Payment is not the same as an unauthorised transaction. For Mistaken Internet Payments, refer to clause 5.16.

## 8.4 When you are liable for EFT transactions

You will be liable for losses in respect of a nominated account caused by an unauthorised EFT transaction, where we prove on the balance of probabilities that the user has contributed to losses:

– 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 code 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 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 record) on the one article, or on several articles liable to be lost or stolen 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 all secret codes; 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, Payment Device or security token, or breach of the security of the secret code. You will also be liable for losses which occur as a result of you 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 the time the user became aware of the unauthorised use, loss or theft (or should reasonably have become aware in the case of a lost or stolen card, Payment Device or security token) and the time we were actually notified. 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) that portion of the loss on a nominated account which exceeds the balance of that nominated account (including any pre-arranged credit); and
d) losses incurred on any accounts which you had not agreed with us could be accessed using the access method.

## 8.5 When your liability for EFT transactions is limited

Where a secret code was required to perform the unauthorised EFT transaction and clause 8.4 does not apply, your liability for any loss in respect of a nominated 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 secret code becoming known to someone else, is the lesser of:

- $150;
- the balance of your nominated account (including any pre-arranged credit); or
- the actual loss at the time we are notified of the misuse, loss or theft of the card or security token, or 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 nominated account).

## 8.6 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 Mastercard scheme rules (or, if relevant, the EFTPOS card scheme rules) against other parties to that scheme.

## 8.7 When the electronic banking system or EFT terminal breaks down

In the event of a terminal malfunction or breakdown, manual procedures may be available by using the card and a signature authorisation procedure (note: this procedure is not available on Virtual card). Your liability for any transaction requiring signature authorisation will be determined in accordance with the Conditions of Use applying to your nominated account.

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 our system or our equipment malfunctions and the user should have been aware that the system or equipment was unavailable for use or malfunctioning, we will only be responsible for correcting errors in your nominated account and refunding any charges or fees imposed on you as a result.

Please advise us if an EFT terminal has a service fault or difficulty. This can be done by messaging us in the Bankwest App or by telephoning our Contact Centre.

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

You have the benefit of certain protections as a consumer under the Australian Consumer Law. Nothing in this document shall be taken to exclude liability which may not be excluded under the Australian Consumer Law. However, to the extent permitted under the Australian Consumer Law and except as otherwise specified in these Conditions of Use, in relation to any loss you have suffered:

- our liability is limited to the cost of providing the relevant services again; and
- we have no liability for any indirect, special or consequential loss (including loss of profits, actual or anticipated revenue).

Part 9

# Liability for Mobile Wallet Transactions

## 9.1 Application of this Part

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

## 9.2 Authorised transactions

You are liable for all transactions carried out in respect of your nominated account with a user's mobile device and a Mobile Wallet including:

– transactions carried out in respect of your nominated account with the knowledge and consent of a user; and

– 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 7.1.

## 9.3 When you are not liable for EFT transactions made using a Mobile Wallet

You will not be liable for losses in respect of a nominated account caused by an EFT transaction made using a Mobile Wallet:

a) resulting from unauthorised use of a card before the user has received the card;

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

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

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

d) where it is clear that the user has complied with all of the security measures described for mobile devices and Mobile Wallets in clause 7.1; or

e) caused by the same transaction being incorrectly debited more than once to the same account.

Part 10

# Payment Device Conditions of Use

## 10.1 About these conditions

Part 10 (together with Parts 1, 7, 8, and 11) 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 to access your nominated account(s).

All references in this Part to "nominated account" are taken to include a reference to "Nominated Account".

## 10.2 All Payment Devices remain our property

Should you request us to issue you with a Payment Device, we grant you a licence to use the Payment Device and may charge you a fee for the manufacture, use and set up of the Payment Device which will be described in the relevant Product Schedule. Unless due to our error, you may be charged the Payment Device fee each time we issue a Payment Device to your nominated account.

All Payment Devices remain our property at all times until:

- you request us to cancel the use of the Payment Device;
- you close your nominated account;
- the expiry of the Payment Device; or
- electronic access to your nominated account has been cancelled in accordance with clause 1.9.

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.

## 10.3 Additional cardholders

If your nominated account permits, you may request us to issue a Payment Device and PIN to an additional cardholder. The relevant provisions of these Conditions of Use apply to the additional cardholder's use of the Payment Device and PIN to access your nominated account.

You are responsible for informing the additional cardholder how to use the Payment Device. We suggest that you provide the additional cardholder with a copy of these Conditions of Use. A copy of these Conditions of Use can be obtained from our website (bankwest.com.au).

You and not the additional cardholder will be liable for all transactions made by the additional cardholder on your nominated account using the Payment Device until the additional cardholder's authority is cancelled.

An additional cardholder's Payment Device is cancelled only when:

- we have received your request to cancel that user's Payment Device; and • we have actioned that request, or we are satisfied, acting reasonably, that the Payment Device is no longer linked to your nominated account.

It is your responsibility to request us to cancel the additional cardholder's Payment Device.

You consent to the additional cardholder having access, in respect of nominated accounts, to information about the account balance, payments, purchases and cash advances.

## 10.4 Use of the Payment Device

In order to use a Payment Device, you (or, if your account is in more than one name, each of you) and each other user will need to activate a Payment Device upon receipt by following the directions that we will provide for that purpose. The Payment Device is valid only for the period indicated on the communication that is given to you at the time of your Payment Device being provided. We will notify you of the expiry of the Payment Device.

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 occurring outside Australia (whether effected in foreign or Australian dollars) we will charge the Foreign Transaction Fee described in the Product Schedule.

## 10.5 Types of transactions that can be made

Transactions 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.

## 10.6 Transactions needing authorisation

Transactions on nominated accounts may need to be authorised by us. We may decline to authorise a transaction if:

- you are behind in making payments to a nominated account;
- (you have an overdraft facility) and the credit limit on a nominated account is exceeded;
- there are insufficient funds in a cheque or savings nominated account; 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.

## 10.7 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 nominated accounts on the day they are made. Processing may take a number of days. We will process transactions to your nominated accounts 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.**

## 10.8 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 or a financial institution 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.

## 10.9 Payment Devices

To the extent permitted by applicable law, including the Australian Consumer Law 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);
- 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, except to the extent caused by our negligence, fraud, wilful misconduct or that of our agents.

Please contact us if you have any questions or concerns in relation to the Payment Device.

Part 11

# Procedures for Handling Errors and Disputed Transactions

The entirety of Part 11 applies to unauthorised transactions and disputed transactions (chargebacks), and reflects our obligations under the ePayments Code. Clauses 11.1 – 11.5 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; or,
- reports of Mistaken Internet Payments under the ePayments Code, which have a separate process set out in clause 5.16. For how to report a Mistaken Internet Payment, see clause 5.16(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).

## 11.1 How to contact us

If you believe a transaction is wrong or unauthorised or you think there is something wrong with an entry on a nominated account statement you may tell us by:

- messaging us in the Bankwest App;
- telephoning our Contact Centre on **13 17 19**;
- logging on to our website (bankwest.com.au) and following the procedures it sets out for disputing a transaction or lodging a complaint; or
- writing to us at the address shown on the nominated account statement containing the suspected error.

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. If you are disputing a transaction, you must tell us immediately using one of the contact methods above. You must complete a Transaction Dispute Form and you should do so promptly. This form can be obtained from our website or messaging us in the Bankwest App. We will notify you of the name and contact number of the officer investigating your dispute.

## 11.2 Chargebacks

This sub-clause 11.2 applies to transactions effected with the Debit Mastercard or Virtual Card (other than those made by selecting the Cheque, Savings or Credit key at an EFT Terminal and entering a PIN to authorise the transaction or a Payment Device, or any transactions otherwise routed through the EFTPOS card scheme). It does not apply to any other type of transaction.

We have the right under the Mastercard scheme rules to seek the reversal of transactions, involving a chargeback or debiting of the 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 debit 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 Mastercard scheme rules. Please note, however, that no Mastercard chargeback right will exist in relation to BPAY payments made using your Debit Mastercard, or Virtual Card or where a transaction is routed through the EFTPOS card scheme. We will use our best efforts to chargeback a disputed transaction for the most appropriate reason. This does not mean that a 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 Mastercard scheme rules. You should make every effort to report a disputed transaction by completing the Transaction Dispute Form 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 time frame could affect our ability to claim a chargeback right (if any) under the Mastercard scheme rules.

These rules impose time limits on reporting disputed transactions, charges, refunds or payments. In certain circumstances where the ePayments Code applies, there may be no such time frames imposed upon your right to make a claim or report a disputed transaction.

## 11.3 Our investigations

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

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 complaint by exercising our rights under the Mastercard scheme rules, within 60 days) of you reporting your matter to us, unless there are exceptional circumstances. In such circumstances, we will write to you and let you know the reasons for the delay and provide you with monthly updates (or, if we resolve your complaint by exercising our rights under the Mastercard scheme rules, updates every two months) 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.

If we resolve your complaint by exercising our rights under the Mastercard scheme rules, we will also 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 charges related to that amount until your complaint has been resolved.

## 11.4 Outcome

If required under the ePayments Code, on completion of our investigation we shall advise you in writing of the outcome of our investigation and the reasons for our decision with reference to the relevant provisions of these Conditions of Use and the ePayments Code.

If we decide that your nominated account has been incorrectly debited or credited we shall adjust your nominated 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 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 nominated 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.

## 11.5 If you are not satisfied with the result

If you are not satisfied with our findings you may request a review by our senior management. Additionally, you may be able to refer the matter (free of charge) to:

**Australian Financial Complaints Authority Limited**

**GPO Box 3 Melbourne, VIC 3001**

**Fax: (03) 9613 6399**

**Telephone: 1800 931 678**

**www.afca.org.au**

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

## 11.6 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 12

# PayTo Service Conditions of Use

## 12.1 About the PayTo Service Conditions of Use

Part 12 (together with Parts 1, 4, 7, 8 and 11) of these Conditions of Use applies to the PayTo Service. The PayTo Service Conditions of Use operate in conjunction with the Conditions of Use applicable to Bankwest Online Banking (see Part 4 above) and to your nominated accounts accessed using these services. The PayTo Service Conditions of Use prevail to the extent of any inconsistency.

We will advise you via Bankwest Online Banking when the PayTo Service becomes available for a particular version of Bankwest Online Banking (e.g. we will advise you via the Bankwest App when the PayTo Service becomes available to the Bankwest App).

Note - for the purposes of these PayTo Service Conditions of Use, a reference to "you" may also include a User (ie an authorised signatory), where relevant. This means that an authorised signatory may also establish, authorise and manage Payment Agreements on an eligible nominated account.

## 12.2 Creating a Payment Agreement

a) The PayTo Service allows payers to establish and authorise Payment Agreements with Merchants or Payment Initiators who offer the PayTo Service as a payment option.

b) If you elect to establish a Payment Agreement with a Merchant or Payment Initiator that offers PayTo payment services, you will be required to provide the Merchant or Payment Initiator with your personal information including BSB/account number or PayID. You are responsible for ensuring the correctness of the account number or PayID you provide for the purpose of establishing a Payment Agreement. Any personal information or data you provide to the Merchant or Payment Initiator will be subject to the privacy policy and terms and conditions of the relevant Merchant or Payment Initiator.

c) Payment Agreements must be recorded in the Mandate Management Service in order for NPP Payments to be processed in accordance with them. The Merchant or Payment Initiator is responsible for creating and submitting a record of each Payment Agreement to their financial institution or payments processor for inclusion in the Mandate Management Service. The Mandate Management Service will notify us of the creation of any Payment Agreement established using your account or PayID details. We will deliver a notification of the creation of the Payment Agreement to you via email (or by post if we do not have your email address), and provide details of the Merchant or Payment Initiator named in the Payment Agreement, the payment amount and payment frequency (if these are provided) to seek your confirmation of the Payment Agreement.
You may confirm or decline any Payment Agreement presented for your approval. If you confirm, we will record your confirmation against the record of the Payment Agreement in the Mandate Management Service and the Payment Agreement will then be deemed to be effective.
If you decline, we will note that against the record of the Payment Agreement in the Mandate Management Service.

d) Subject to clause 12.7 (which address Migration of Direct Debit arrangements), we will process payment instructions in connection with a Payment Agreement, received from the Merchant's or Payment Initiator's financial institution, only if you have confirmed the associated Payment Agreement. Payment instructions may be submitted to us for processing immediately after you have confirmed the Payment Agreement so you must take care to ensure the details of the Payment Agreement are correct before you confirm them. We will not be liable to you or any other person for loss suffered as a result of processing a payment instruction submitted under a Payment Agreement that you have confirmed.

e) If a Payment Agreement requires your confirmation within a timeframe stipulated by the Merchant or Payment Initiator, and you do not provide confirmation within that timeframe, the Payment Agreement may be withdrawn by the Merchant or Payment Initiator.

f) If you believe the payment amount or frequency or other detail presented is incorrect, you may decline the Payment Agreement and contact the Merchant or Payment Initiator and have them amend and resubmit the Payment Agreement creation request.

## 12.3 Amending a Payment Agreement

a) Your Payment Agreement may be amended by the Merchant or Payment Initiator from time to time, or by us on your instruction.

b) We will send you notification/s of proposed amendments to the payment terms of the Payment Agreement requested by the Merchant or Payment Initiator. Such amendments may include variation of the payment amount, where that is specified in the Payment Agreement as a fixed amount, payment frequency or Payment Agreement end date. The Mandate Management Service will notify us of the amendment request. We will notify you via email (or by post if we do not have your email address) that you have received an amendment request, and we will provide you with instructions on how you can review and respond to that request. You may confirm or decline any amendment request presented for your approval. If you confirm, we will record the confirmation against the record of the Payment Agreement
in the Mandate Management Service and the amendment will then be deemed to be effective. If you decline, the amendment will not be made. A declined amendment request will not otherwise affect the Payment Agreement.

c) Amendment requests which are not confirmed or declined within 5 calendar days of being sent to you, will expire. If you do not authorise or decline the amendment request within this period of time, the amendment request will be deemed to be declined.

d) If you decline the amendment request because it does not reflect the updated terms of the agreement that you have with the Merchant or Payment Initiator, you may contact them and have them resubmit the amendment request with the correct details. We are not authorised to vary the details in an amendment request submitted by the Merchant or Payment Initiator.

e) Once an amendment request has been confirmed by you, we will promptly update the Mandate Management Service with this information.

f) Once a Payment Agreement has been established, you may instruct us to amend only your account details in the Payment Agreement only. Account details may only be replaced with the BSB and account number, or PayID, of an account you hold with us. If you wish to amend the account details to refer to an account with another financial institution, you may give us a transfer instruction see clause 12.5. We may decline to act on your instruction to amend your Payment Agreement if we are not reasonably satisfied that your request
is legitimate. You may not request us to amend the details of the Merchant or Payment Initiator, or another party.

## 12.4 Pausing your Payment Agreement

a) You may instruct us to pause and resume your Payment Agreement via Bankwest Online Banking (via the Bankwest App or desktop) or by phone. We will act on your instruction to pause or resume your Payment Agreement promptly by updating the record of the Payment Agreement in the Mandate Management Service. However, where a Payment Agreement has been paused due to fraud concerns, we may not act on your instruction to resume the Payment Agreement until fraud concerns have been adequately addressed. The Mandate Management Service will notify the Merchant's or Payment Initiator's financial institution or payment processor of the pause or resumption. During the period the Payment Agreement is paused, we will not process payment instructions in connection with it. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator.

b) Merchants and Payment Initiators may pause and resume their Payment Agreements. If the Merchant or Payment Initiator pauses a Payment Agreement to which you are a party, we will promptly notify you of that, and of any subsequent resumption, via email (or by post if we do not have your email address). Payment Agreements that have been paused by a Merchant or Payment Initiator cannot be resumed by you. Should you wish to resume the Payment Agreement you will need to contact the Merchant or Payment Initiator to request them to do so. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement by the Merchant or Payment Initiator.

## 12.5 Transferring your Payment Agreement

a) When we advise you of the availability of this functionality, you may elect to have payments under your Payment Agreement made from an account at another financial institution. You may do this by contacting us via Bankwest Online Banking (via the Bankwest App or desktop) and selecting "Transfer your Payment Agreement", or by phone. We will provide you with a Transfer ID to provide to your new financial institution to enable them to complete the transfer.

b) Your new financial institution will be responsible for having you authorise the transfer of the Payment Agreement and also updating the Payment Agreement in the Mandate Management Service. The updated Payment Agreement will become effective upon being updated in the Mandate Management Service.

c) Until the Transfer is completed, the Payment Agreement will remain linked to your account with us. If the other financial institution does not complete the transfer within 14 calendar days, the transfer will be deemed to be ineffective and payments under the Payment Agreement will continue to be made from your account with us.

d) To Transfer a Payment Agreement that you have with another financial institution to us, you will need to obtain a Transfer ID from that institution and provide it to us by via Bankwest Online Banking (via the Bankwest App or desktop). Where you instruct us to process a Transfer of a Payment Agreement from another financial institution to us, we will use reasonable endeavours to do so within 14 days. We do not guarantee that all Payment Agreements will be transferrable to us. If we are unable to complete a Transfer, we will notify you and advise you of your options.

## 12.6 Cancelling your Payment Agreement

a) You may instruct us to cancel a Payment Agreement on your behalf via Bankwest Online Banking (via the Bankwest App or desktop) or by phone. We will act on your instruction promptly by updating the record of the Payment Agreement in the Mandate Management Service. However, where a Payment Agreement has been paused due to fraud concerns, we may not act on your instruction to cancel the Payment Agreement until fraud concerns have been adequately addressed. The Mandate Management Service will notify the Merchant's or Payment Initiator's financial institution or payment processor of the cancellation. You will be liable for any loss that you suffer as a result of the cancellation of a Payment Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator (for example, any termination notice periods that have not been adhered to), or if a cancellation fee is imposed by the Merchant or Payment Initiator.

b) Merchants and Payment Initiators may cancel Payment Agreements. If the Merchant or Payment Initiator cancels a Payment Agreement to which you are a party, we will promptly notify you of that cancellation via email (or by post if we do not have your email address). We will not be liable to you or any other person for loss incurred as a result of the cancellation of your Payment Agreement by the Merchant or Payment Initiator.

c) Payment Agreements that have been cancelled cannot be resumed.

## 12.7 Migration of Direct Debit arrangements

a) Merchants and Payment Initiators who have existing Direct Debit arrangements with their customers, may establish Payment Agreements for these, as Migrated DDR Mandates, in order to process payments under those arrangements via the NPP rather than BECS (the Bulk Electronic Clearing System). If you have an existing Direct Debit arrangement with a Merchant or Payment Initiator, you may be notified by them that future payments will be processed from your account under the PayTo Service. You are entitled to prior written notice of variation of your Direct Debit arrangement and changed processing arrangements, as specified in your Direct Debit Service Agreement, from the Merchant or Payment Initiator. If you do not consent to the variation of the Direct Debit arrangement you must advise the Merchant or Payment Initiator. We are not obliged to provide notice of a Migrated DDR Mandate to you for you to confirm or decline. We will process instructions received from a Merchant or Payment Initiator on the basis of a Migrated DDR Mandate unless you indicate to us not to. Our processing will commence at least 5 days after we received the instructions from the Merchant or Payment Initiator.

b) You may amend, pause (and resume), cancel or transfer your Migrated DDR Mandates, or receive notice of amendment, pause or resumption, or cancellation initiated by the Merchant or Payment Initiator, in the manner described in clauses 12.3 – 12.6.

c) If a Migrated DDR Mandate is amended, the daily payment authorisation limit applying to your PayTo Service will apply.

## 12.8 Your responsibilities

a) You must ensure that you carefully consider any Payment Agreement creation request, or amendment request made in respect of your Payment Agreement or Migrated DRR Mandates and promptly respond to such requests. We will not be liable for any loss that you suffer as a result of any payment processed by us in accordance with the terms of a Payment Agreement or Migrated DDR Mandate.

b) You must notify us immediately if you no longer hold or have authority to operate the account from which payments under a Payment Agreement or Migrated DDR Mandate have been /will be made.

c) You must promptly respond to any notification thatyou receive from us regarding the pausing or cancellation of a Payment Agreement or Migrated DDR Mandate for misuse, fraud or for any other reason. We will not be responsible for any loss that you suffer as a result of you not promptly responding to such a notification.

d) You are responsible for ensuring that you comply with the terms of any agreement that you have with a Merchant or Payment Initiator, including any termination notice periods. You acknowledge that you are responsible for any loss that you suffer in connection with the cancellation or pausing of a Payment Agreement or Migrated DDR Mandate by you which is in breach of any agreement that you have with that Merchant or Payment Initiator.

e) You are responsible for ensuring that you have sufficient funds in your account to meet the requirements of all your Payment Agreements and Migrated DDR Mandates. Subject to any applicable laws and binding industry codes, we will not be responsible for any loss that you suffer as a result of your account having insufficient funds. The terms and conditions applying to your account, which are available at www.bankwest.com.au will apply in relation to circumstances where there are insufficient funds in your account.

f) If you receive a Payment Agreement creation request or become aware of payments being processed from your account that you are not expecting, or experience any other activity that appears suspicious or erroneous, please report such activity to us via phone or in writing promptly.

g) From time to time you may receive a notification from us via email (or by post if we do not have your email address) requiring you to confirm that all of your Payment Agreements and Migrated DDR Mandates are accurate and up to date. You must promptly respond to any such notification. Failure to respond may result in us pausing the Payment Agreement/s or Migrated DDR Mandate/s.

h) If you use Bankwest Online Banking (via the Bankwest App or desktop) to do your banking, we recommend that you allow notifications from Bankwest Online Banking to ensure that you're able to receive and respond to Payment Agreement creation requests, amendment requests and other notifications in a timely way.

i) In using the facilities that we provide to you in connection with establishing and managing your Payment Agreements and Migrated DDR Mandates, you are required:

   i) not to engage in unsatisfactory account operation (as described in this Account Access Conditions of Use document and, where relevant, our Investment and Transaction Account Terms and Conditions – each available at www.bankwest.com.au);

   ii) to ensure that all data you provide to us or to any Merchant or Payment Initiator that subscribes to the PayTo Service is accurate and up to date; and

   iii) to otherwise comply with your contractual obligations - including in connection with maintaining the confidentiality of the security of your access to facilities we provide (e.g. Password and PIN).

j) All intellectual property, including but not limited to the PayTo Service logo and all documentation, remains our property, or that of our licensors (Our Intellectual Property). We grant to you a royalty free, non-exclusive license (or where applicable, sub-license) for the term to use Our Intellectual Property for the sole purpose of using the PayTo Service in a way that is consistent with the terms of this agreement within Australia.

k) Where an intellectual property infringement claim is made against you, we will have no liability to you under this agreement to the extent that any intellectual property infringement claim is based upon:

   i) modifications to Our Intellectual Property by or on behalf of you in a manner that causes the infringement;

   ii) use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item;

   iii) your failure to use corrections or enhancements to Our Intellectual Property that are made available to you (except where the use of corrections or enhancements would have caused a defect in the Mandated Payments Service or would have had the effect of removing functionality or adversely affecting the performance of the Mandated Payments Service); and

   iv) your failure to use Our Intellectual Property in accordance with this agreement.

l) You must comply with all applicable laws in connection with your use of the PayTo Service.

## 12.9 Our responsibilities

a) We will accurately reflect all information you provide to us in connection with a Payment Agreement or a Migrated DDR Mandate in the Mandate Management Service.

b) We may monitor your Payment Agreements or Migrated DDR Mandates for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreement or Migrated DDR Mandates if we reasonably suspect misuse, fraud or security issues. We will promptly notify you via email (or by post if we do not have your email address) of any such action to pause or cancel your Payment Agreement.

c) If you become aware of a payment being made from your account, that is not permitted under the terms of your Payment Agreement or Migrated DDR Mandate or that was not authorised by you, please contact us as soon as possible via the methods set out in Part 11 and submit a claim. We will respond to all claims within one business day. If the claim is founded, we will refund your account. We will not be liable to you for any payment made that was in fact authorised by the terms of your Payment Agreement or Migrated DDR Mandate.

bankwest.com.au

BWA-A30_280525

Bankwest, a division of Commonwealth Bank of Australia
ABN 48 123 123 124 AFSL / Australian Credit Licence 234945.

Version 37 | 28 May 2025