Account & Access Facility
Conditions of Use

THIS DOCUMENT MUST BE READ TOGETHER WITH REGIONAL AUSTRALIA BANK's:

- Fees and Charges
- Summary of Accounts and Availability of Access Facilities

Together these brochures form the Conditions of Use for the Regional Australia Bank's Account and Access Facilities.

If you have not received all three parts, please contact the Regional Australia Bank on 132 067 or visit our website.

You should read all three parts before deciding to open Accounts and Access Facilities

Effective Date: 13 October 2026

Regional Australia Bank Accounts are issued by:
Regional Australia Bank Ltd ABN 21 087 650 360
AFSL and Australian Credit Licence 241167

How To Contact Us

Visit us at any of our branches – visit our website at regionalaustraliabank.com.au for our branch details

- ☎ Phone us on 132 067
- ✉ Write to us at:
  PO Box U631
  ARMIDALE NSW 2351
- 🖷 Email us on enquiries@regionalaustraliabank.com.au

☞ **To report the loss, theft or unauthorised use of your Visa please visit our website.**

Customer Owned Banking Code of Practice

We warrant that we will comply with the Customer Owned Banking Code of Practice. Please see the section About the Customer Owned Banking Code of Practice at the end of these Conditions of Use for more detail.

ePayments Code

We warrant that we will comply with the ePayments Code.

How Our Conditions of Use Become Binding On You

Please note that by opening an Account or using an access facility you become bound by these Conditions of Use.

This document should be read together with the Summary of Accounts and Access Facilities brochure and the Fees and Charges brochure.

Accessing Copies of the Conditions of Use

Please keep these Conditions of Use in a safe place so you can refer to it when needed. Alternatively, you can view and download our current Conditions of Use from our website at regionalaustraliabank.com.au

The Financial Claims Scheme

The Financial Claims Scheme (FCS) is an Australian Government scheme that protects depositors through the provision of a guarantee on deposits held in authorised deposit taking institutions (ADIs) incorporated in Australia and allows quick access to their deposits in an ADI in the unlikely event that one of these financial institutions fails. Regional Australia Bank is an ADI.

Under the FCS deposits with Regional Australia Bank are protected up to a limit of $250,000 for each Account holder.

The FCS can only come into effect if it is activated by the Australian Government when an institution fails. Once activated, the FCS will be administered by the Australian Prudential Regulation Authority (APRA).

The FCS limit of $250,000 applies to the sum of an Account holder's deposits under the one banking license.

Therefore, all deposits held by an Account holder with a single banking institution must be added together towards the $250,000 FCS limit, and this includes Accounts with any other banking businesses that the licenced banking institution may operate under a different trading name.

For further information about the FCS visit the FCS website – www.fcs.gov.au.

TABLE OF CONTENTS

Account Operations 1
Complaints 6
Chequing 6
Direct Debit 7
Electronic Access Facilities & ePayments Conditions Of Use 7
Section 1. Information About our ePayments Facilities 7
Section 2. Definitions 10
Section 3. Transactions 12
Section 4. How To Report Loss, Theft Or Unauthorised Use Of Your Card or Pass Code 12
Section 5. How to Report Unauthorised Use Of Online Banking Services 12
Section 6. ePayments Transaction Limits 12
Section 7. Processing ePayments Transactions 13
Section 8. Using Online Banking Services 13
Section 9. Mistaken Internet Payments 13
Section 10. Using BPAY® 14
Section 11. Processing BPAY® Payments 15
Section 12. Future-Dated BPAY® Payments 15
Section 13. Consequential Damage For BPAY® Payments 15
Section 14. Using A Visa Card 16
Section 15. Using A Visa Card Outside Australia 16
Section 16. Additional Visa Card 16
Section 17. Using Visa Card To Make Deposits At ePayment Terminals 16
Section 18. Use After Cancellation Or Expiry Of The Visa Card 16
Section 19. Exclusions Of Visa Card Warranties And Representations 16
Section 20. Your Liability For ePayments Transactions 17
Section 21. Malfunction 17
Section 22. Cancellation Of Visa Card Or Of Access To Online Banking Services, BPAY® or PayTo 18
Section 23. Visa Secure 18
Section 24. Additional Cardholders and visa Secure 18
Section 25. Termination of Visa Secure 18
Section 26. Participating Online Merchant 18
Section 27. Exclusion of Liabilities and visa secure 19
Section 28. Your conduct and visa secure 19
Section 29. Privacy and visa secure 19
Section 30. Click to Pay 19
Section 31. Regular Payment Arrangements 19
Section 32. Making and Receiving NPP Payments Using PayID 20
Section 33. Using Osko® 21
Section 34. Processing Osko® Payments 21
Section 35. Scheduled and Recurring Osko® Payments 22
Section 36. Authority to Recover Mistaken or Misdirected NPP Payments 22
Section 37. Creating a PayTo Payment Agreement 22
Section 38. Amending a Payment Agreement 22
Section 39. Pausing your Payment Agreement 23
Section 40. Transferring your Payment Agreement 23
Section 41. Cancelling your Payment Agreement 23
Section 42. Migration of Direct Debit arrangements 23
Section 43. General PayTo Provisions 24
Section 44. Privacy and PayTo 25
Section 45. Authority for PayTo Instructions 25
Section 46. Confirmation of payee 25
Section 47. Misuse of payment description and transaction messaging 25
Section 48. Information sharing (including personal information) 26
About the Customer Owned Banking Code of Practice 26

ACCOUNT OPERATIONS

WHAT IS THE REGIONAL AUSTRALIA BANK ACCOUNT AND ACCESS FACILITY?

A Regional Australia Bank Account (**Account**) gives you transaction, savings and term savings functionality. These Accounts can be accessed through the use of the below access facilities:

- Visa Card
- chequing
- BPAY® (registered to BPAY Pty Ltd ABN 69 079 137 518)
- Osko® Payments
- Payto
- phone banking
- internet banking and Mobile Device App
- EFTPOS and ATM access
- direct debit requests
- Bank@Post
- Digital Wallet

(**Access Facilities**)

Please refer to the *Summary of Accounts & Availability of Access Facilities* brochure for available Account types, the conditions applying to each Account type and the access method attached to each Account type.

HOW DO I OPEN AN ACCOUNT?

You will need to become a Member or Customer of Regional Australia Bank before we can open an Account for you.

To become a Member or a Customer, you will need to complete an application (this can be done in branch, over the phone or via our website)

To become a Member you will need to subscribe for a Member share in Regional Australia Bank. Customers are not required to subscribe for a Member share in Regional Australia Bank.

As Members of Regional Australia Bank are shareholders they are entitled to vote at the Regional Australia Bank annual general meetings. Customers do not hold a member share and are not entitled to vote at Regional Australia Bank's annual general meetings.

PROOF OF IDENTITY REQUIRED

The law requires us to verify your identity when you open an Account or the identity of any person you appoint as a signatory to your Account.

In most cases you can prove your identity by showing us one of the following photo identity documents:

- current photo driver's licence issued by a State or Territory or foreign government
- current photo card issued by a State or Territory government
- current passport (or expired within last 2 years) issued by the Commonwealth
- passport, with photo of the person, issued by a foreign government, the United Nations, or a UN agency - if not in English - accompanied by an English translation prepared by an accredited translator
- national ID card, with photo and signature of the person, issued by a foreign government, the United Nations, or a UN agency - if not in English - accompanied by an English translation prepared by an accredited translator
- firearms licence issued by a state or territory

NOTE ABOUT CERTIFYING TRANSLATIONS OF DOCUMENTS NOT IN ENGLISH:

If a document is written in a language that is not understood by the person carrying out the identification procedure, then it has to be accompanied by an English translation prepared by an accredited translator.

If you do not have photo ID please contact us to discuss what other forms of identification may be acceptable.

The law does not allow you to open an Account using an alias without you also giving us all the other names that you are commonly known by.

If you want to appoint a signatory to your Account, the signatory will also have to provide proof of identity, as above.

WHAT ACCOUNTS CAN I OPEN?

When your application to become a Member or a Customer is approved by Us, you will have access to a transaction Account. You can then activate other Accounts as needed. Please first check the *Summary of Accounts & Availability of Access Facilities* brochure for the different Account types available, any special conditions for opening, and the features and benefits of each Account type.

TRUST ACCOUNTS

You can open an Account as a trust Account. However:

- we are not taken to be aware of the terms of the trust;
- we do not have to verify that any transactions you carry out on the Account are authorised by the trust.

You agree to indemnify us against any claim made upon us in relation to, or arising out of that trust.

TERM DEPOSIT ACCOUNTS

You can make a deposit that guarantees an agreed interest rate on that deposit for the term you choose. You can speak to our staff or refer to our website for the Schedule of Interest Rates available on any term deposit Accounts.

If we quote you an interest rate for a term deposit Account, the rate may differ if the deposit is not made on the same day as the quote.

Interest on term deposits remains fixed for the agreed term of the deposit. Interest is calculated daily and paid as agreed at the time of investment of funds either fortnightly, monthly, quarterly, yearly or at maturity depending on the term of the investment.

When your term deposit falls due we will contact you to advise you of your options. If you do not provide instructions in relation to the particular term deposit on or before the maturity date, we will automatically reinvest the principal for a similar term at the then current rate. Interest will be paid in the same manner as last advised.

Transactions may not be processed on the same day that the term deposit matures should that date not be a business day. In such cases the transaction will be processed the next business day.

Funds may be withdrawn prior to maturity, however an early redemption interest adjustment and

administration fee will apply. If any interest has been paid prior to the early redemption of a term deposit, any shortfall arising from the recalculation of interest in accordance with the early redemption will be deducted from the principal amount.

If you change your mind, we provide a grace period of 14 calendar days, starting on the date of deposit. If you would like to withdraw or transfer your investment to a different term, please contact us to arrange this during this grace period.

MORTGAGE OFF SET ACCOUNT

A mortgage offset Account provides 100% offset of the balance of your Mortgage Offset Account against the interest payable on your Offset Loan.

A mortgage offset Account can only be offset against a loan with offset features (**Offset Loan**), if the Account and the home loan are in the name of the same person or persons. This means that:

(a) Joint Offset accounts can be linked to a Joint Offset Loan.

(b) Single Offset accounts can be linked to a Single Offset Loan; and

(c) Single Offset accounts can be linked to a Joint Offset loan.

The mortgage offset Account has a maximum of 8 Accounts and sub-Accounts that can be used in the method of calculation of interest against the Mortgage Offset Loan Account. This will mean that:

(a) interest is calculated on the daily balance of your mortgage offset Account and charged to the Offset Loan monthly; and

(b) there will be no minimum monthly balance to maintain in your Mortgage Offset Accounts.

No interest will be earnt on the balance of your mortgage Offset Accounts even if the Offset Loan is repaid in full.

The mortgage offset Account operates as a variation of the method of calculation of interest under your Offset Loan contract as follows:

(i) the Offset Loan is only available on owner occupied Offset Loans or residential investment loans where the borrower is a natural person, with a variable interest rate;

(ii) when calculating interest on your Offset Loan, the unpaid balance used for the calculation of interest will be reduced by the balance of your Mortgage Offset Accounts (**Offset Balance**);

(iii) the Offset Balance is calculated by multiplying the balance of your Mortgage Offset Accounts at the end of the day by the interest rate payable on the Offset Loan.

WHAT FEES AND CHARGES ARE THERE?

Please refer to the *Fees and Charges* brochure for current fees and charges. We may vary fees or charges from time to time.

We will debit your primary operating Account for all applicable government taxes and charges and any fees.

WHAT INTEREST CAN I EARN ON MY ACCOUNT?

The Interest Rates page on our website provides information about our current deposit, savings and loan interest rates. We may vary our interest rates from time to time. Such variations will not impact existing term deposits until the then current maturity date.

Please refer to our Summary of Accounts & Availability Access Facilities brochure or your current loan contract to see how we calculate and credit or debit interest to your Account.

WHAT ARE THE TAXATION CONSEQUENCES?

Interest earned on an Account is income and may be subject to income tax.

DISCLOSING YOUR TAX FILE NUMBER

When you apply for an Account with Regional Australia Bank we will ask you whether you want to disclose your Tax File Number (TFN) or exemption. If disclosed, we will note your TFN or exemption against each active Account that you hold with Regional Australia bank at that time.

You do not have to disclose your TFN to us. If you choose not to disclose your TFN, we are required to deduct withholding tax from any interest earned on your Account at the highest marginal rate of tax.

For a joint Account, each holder must quote their TFN and/or exemptions, otherwise withholding tax applies to all interest earned on the joint Account.

For business Accounts and charities, you need only quote your Australian Business Number.

THIRD PARTY ACCESS

You can authorise us at any time to allow another person to operate on your Accounts. However, we will need to verify this person's identity before they can access your Account.

You can specify which of your Accounts you give the authorised person authority to operate on. You are responsible for all transactions your authorised person carries out on your Account. You should ensure that the person you authorise to operate on your Account is a person you trust fully.

Note: When you authorise a person to operate on your Accounts, they will also become your nominated representative under any Consumer Data Right Authorisations which will allow that person to amend, create or manage any Consumer Data Right consents. Please refer to our Consumer Data Rights Policy available on our website. You may revoke the authorised person's authority at any time by giving us written notice.

MAKING DEPOSITS TO YOUR ACCOUNT

You can make deposits to an Account:

- by cash or cheque at any branch
- by direct credit eg from your employer for wages or salary – please note that we can reverse a direct credit if we do not receive full value for the direct credit
- by transfer from another Account with us
- by transfer from another financial institution
- via Australia Post Bank@Post.

Note that electronic deposits may not be processed on the same day. Please refer to EFT Conditions of Use: Section 7, on page 13.

HOW LONG DOES IT TAKE TO CLEAR A CHEQUE?

When a cheque is deposited to an Account, funds cannot be withdrawn until proceeds have been made available (cleared).

Funds will be made available as follows:

- A cheque drawn on an Australian financial institution – three (3) business days.

- A cheque drawn on an overseas financial institution – forty-five (45) business days.
- When a cheque is deposited via Bank@Post, - seven (7) business days.

Note: there may be a 24-hour extension on the above clearance periods due to the paying bank's chequing procedures. During this period, you will not be able to withdraw any of the proceeds of that cheque.

However, there are some exceptions which allow you immediate access to the proceeds of the cheque. Please check with us as to these circumstances. Also, when depositing the cheque, you can ask us for a special clearance on the cheque. We will tell you how long it will take to specifically clear and the amount of any special clearance fee.

JOINT ACCOUNTS

You may open a joint account with another person over the age of 14.

When opening the Account, you must nominate how you would like the joint Account to be operated. You may elect for the joint Account:-

- To operate jointly, that is two or more signatories must act together and provide joint instructions; or
- To operate severally, that is any signatory can operate on their own without the authorisation of the joint Account holders.

This nomination can change at any time on the instruction of any one or more joint Account holders.

Important Information about Joint Accounts

- The balance of the joint account is held jointly by all account holders;
- The liability of joint account holders on an account is joint and several, that means that if the joint Account becomes overdrawn each of the Account holders may be liable for part or all of the overdrawn amount;
- If there is a dispute relating to a joint Account, we may, suspend or freeze the account (including any re-draw on a credit Account) until we are notified by all Account holders of the resolution of the dispute. In the event that one joint account holder passes away, the ownership of the Account and or any liability for the Account will transfer to the surviving Member or Customer.

WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT

You can make or authorise withdrawals or transfers from your Account:

- over the counter at any branch
- by direct debit
- by cheque, if your Account is linked to a cheque book
- via phone banking
- via internet banking or the Mobile Banking App
- via BPAY® and Osko® to make a payment to a biller
- by Payto
- at ATMs, if your Account is linked to a Visa Card
- via payWave at selected terminals
- via EFTPOS terminals, if your Account is linked to a Visa Card (note that merchants may impose restrictions on withdrawing cash)
- via Australia Post Bank@Post

unless otherwise indicated in the Conditions of Use.

We will require acceptable proof of your identity before processing withdrawals in person or acceptable proof of your authorisation for other types of withdrawal transactions.

We will also require acceptable proof of the identity of any person that you authorise to withdraw funds in person on your behalf.

Debiting Transactions Generally

We will debit transactions received on any one day in the order we determine in our absolute discretion.

We have the right to decline to accept your authorisation for any transaction if there are insufficient funds in your Account, if we are uncertain for any reason of the authenticity or validity of the authorisation or your legal capacity to give authorisation. We may also delay or not process a transaction for any of the reasons set out in Closing Accounts, Cancelling Access Facilities & Delaying, Blocking, Freezing or Refusing Transactions. We will not be liable to you or any other person for any loss or damage which you or such other person may suffer as a result of our action.

If you close your Account before a transaction debit is processed, you will remain liable for any dishonour fees incurred in respect of the transaction.

Re-Draw

If you make early or additional repayments to a loan for which redraw is available and all your loan conditions are satisfied at the time you wish to make a redraw, you can redraw up to the amount by which the total repayments you have made exceed the total repayments required under your loan, less the amount of one loan repayment as set out in the schedule on your loan contract.

Any redraw amount will be debited to your loan account and will form part of the outstanding balance on which debit interest will accrue.

The amount that you redraw can only be cleared funds.

Payments made prior to or during a fixed period are not available to be redrawn at any time during the fixed period.

Each borrower is liable for each redraw (whether or not they are aware of, or authorised, the redraw), in addition to each of you being jointly liable with each other.

Over The Counter Withdrawals

Generally, you can make over-the-counter withdrawals in cash or by purchasing a Financial Institution Cheque. The daily in branch cash withdrawal limit is $5,000.00. You are required to provide 48 hours notices for in branch cash withdrawals greater that this amount. Please check the Summary of Accounts & Availability of Access Facilities brochure for any restrictions on withdrawals applying to certain Accounts.

Withdrawals Using Our Financial Institution Cheques

This is a cheque we draw payable to a person or entity you nominate. You can purchase a Financial Institution Cheque from us for a fee. Please refer to our Fees and Charges brochure.

If a Financial Institution Cheque is lost or stolen, you can ask us to stop payment on it by calling us on 132 067. We may charge a fee to stop payment on a Financial Institution Cheque. Please refer to our Fees and Charges brochure.

We cannot stop payment on a Financial Institution Cheque if you used the cheque to buy goods or services and you are not happy with them. You must seek compensation or a refund directly from the provider of the goods or services. You should contact a Government Consumer Agency if you need help.

Transaction Limits

We limit the amount of daily withdrawals or payments you may make using electronic methods, either generally or in relation to a particular facility. These transaction limits are set out in the Fees and Charges brochure.

At our discretion We may impose a transaction limit of ten thousand dollars ($10,000.00) per transaction or a total of per ten thousand dollars ($10,000.00) calendar month, , to any merchants that we believe may be owned or controlled by a cryptocurrency or digital asset exchange, or being used to purchase cryptocurrency or digital assets. Other financial institutions may impose additional restrictions on the amount of funds that you can withdraw, pay or transfer.

We may also require you to apply for new transaction limits if you change any pass code. We will require you to provide proof of identity that satisfies us. We may reduce transaction limits at any time for security reasons.

Overdrawing An Account

You must keep sufficient cleared funds in your Account to cover your cheque, direct debit and electronic funds transfer (**EFT**) transactions (including PayTo payments). If you do not, we can dishonour the transaction and charge dishonour fees. Please refer to our Fees and Charges brochure.

Cleared funds means the proceeds of cheque deposits to your Account, once the cheque is cleared, cash deposits and direct credits.

Alternatively, we can honour the transaction and overdraw your Account. If this is to occur we may charge you:

- interest at our current overdraft rate, calculated on the daily closing balance; or
- a fee for each day (or part of a day) your Account is overdrawn. Please refer to our Fees and Charges brochure.

Sweep Facility

You may nominate an Account (the first Account) which is to have either a nominated minimum balance or to be maintained in credit. You may then nominate a second Account, which authorises us to transfer, automatically, sufficient funds to keep the first Account at its nominated balance or in credit. However, we are not obliged to transfer funds if there are insufficient funds in the second Account to draw on.

Account Statements

We will send you Account statements at least every 6 months.

When you register for internet banking we will automatically make your statements available via Regional Australia Bank's internet banking platform and we will send you an email using the email you have provided to advise you when your statement(s) become available.

You can also request to receive your Account statements in paper form.

You can ask us for an Account statement at any time. We may charge a fee for providing this statement or an additional statement(s) or copies. Please refer to the Fees and Charges brochure.

We recommend that you check your Account statement as soon as you receive it and immediately

notify us of any unauthorised transactions or errors. Please refer to How to Contact Us on page 1 for our contact details.

WHAT HAPPENS IF I CHANGE MY NAME OR ADDRESS?

You must notify us if you change your name or address.

You can update your name in our branch (evidence of your change of name will be required to be provided).

You can update your address in branch, over the phone, through our internet banking platform or via our Mobile Banking App.

INACTIVE ACCOUNTS

If no transactions are carried out on your Account during a consecutive 12 month period (other than transactions initiated by us, such as crediting interest or debiting fees and charges) we will write to you asking if you want to keep the Account open. If you do not reply within 10 business days of the date of our notice to you, we will treat your Account as being inactive.

To re-activate your account, you can:

- Make a transaction on your account;
- Log into your account via internet or mobile banking; or
- Call us or visit any of our branches.

Once your Account becomes inactive, and in each consecutive 12 month period that your Account remains inactive, we will charge an inactive fee. Please refer to our Fees and Charges brochure.

If your account remains inactive for a period of three (3) years, we will resign your membership, close your account and transfer the funds to a holding ledger. WE will also send you a statement of your account once your accounts have been closed.

We will notify you 30 days before closing your account, but there may be circumstances where we are unable to do so (such as where our record of your contact details is out of date).

Once your membership has been resigned and account closed, we will stope sending you statements of your account. Fees and charges may still apply to inactive accounts.

If your Account remains inactive for 7 years, we have a legal obligation to remit balances exceeding $500.00 to the Australian Securities and Investments Commission as unclaimed money.

ACCOUNT COMBINATION

If you have more than one Account with us, we may apply a deposit balance in any Account to any other Account in the same name which is overdrawn or, to a loan Account if that Account is in arrears.

If you are no longer eligible to be a Customer or your membership is terminated we may combine all your Accounts (whether deposit or loan Accounts) you have with us provided the Accounts are all in the same name.

We will not combine Accounts if to do so would breach the Code of Operation for Services Australia Direct Credit Payments and any successor Code (both when enforcing indebtedness owed to us and, to the law permits, when facilitating enforcement by a third party judgement creditor).

We will give you written notice promptly after exercising any right to combine your Accounts.

CLOSING ACCOUNTS, CANCELLING ACCESS FACILITIES & DELAYING, BLOCKING, FREEZING OR REFUSING TRANSACTIONS

You can close your Account on request at any time. However, you will have to surrender your cheque book and any Visa card linked to the Account at that time. We may defer closure and withhold sufficient funds to cover payment of outstanding debits on the Account.

You can cancel any Access Facility on request at any time.

We can close the Account in our absolute discretion by giving you at least 14 days' notice.

However, without prior notice, we can close, or suspend your access to, any Account, cancel any access facility, or delay, block, freeze or refuse any transaction:

- if we reasonably believe doing so will protect you or us from harm or loss;
- if we reasonably suspect fraudulent or illegal use of the Account or access facility;
- if we reasonably suspect that a transaction may breach a law or sanction;
- If we identify that the transaction is for the purposes of Gambling and you are under the age of eighteen (18);
- to comply with our legal and regulatory obligations, including with our related policies and procedures; or
- if you fail to provide us with information or documents we reasonably request.

We will act fairly and reasonably towards you when taking such action without prior notice.

If we close your Account, we will pay you the net credit balance in the account unless we reasonably believe that our legal or regulatory obligations prevent us from doing so and subject to our right to combine accounts (see ACCOUNT COMBINATION).

NOTIFYING CHANGES

We may change fees, charges, interest rates and other conditions applicable to the Account & Access Facility at any time. We will act reasonably in making these changes and only do so for legitimate business purposes. If you do not like the change, you can ask us to close your Account and Access Facility, or close any account or cancel any access facility in it, in accordance with these Conditions of Use: see CLOSING ACCOUNTS, CANCELLING ACCESS FACILITIES & DELAYING, BLOCKING, FREEZING OR REFUSING TRANSACTIONS. The following table sets out how we will notify you of any change.

Type of change	Notice
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days

Type of change	Notice
Reducing the number of fee-free transactions permitted on your Account	20 days
Changing the minimum balance to which an Account keeping fee applies	20 days
Changing the method by which interest is calculated	20 days
Changing the circumstances when interest is credited to your Account	20 days
Changing interest rates	on the day of change
Increasing your liability for losses relating to ePayments (see the ePayments Conditions of Use for a list of ePayments)	20 days
Imposing, removing or changing any periodic transaction limit	20 days

For all other changes, we will provide reasonable notice (which, depending on the nature of the change, may be before or after the change is made). If we reasonably consider that such a change is unfavourable to you, we will provide at least 20 days' notice. However, we may give shorter, or no, advance notice of a change unfavourable to you if it is reasonable for us to manage a material and immediate risk.

We may use various methods, and combinations of methods, to notify you of these changes, such as:

- notification by letter;
- notification on or with your next statement of Account;
- notification on or with the next newsletter;
- advertisements in the local or national media;
- notifications through internet banking;
- notifications through the Mobile Banking App;
- notifications via email alerts;
- notification via sms; or
- notification on our website.

However, we will always select a method or methods we reasonably consider appropriate to the nature and extent of the change, as well as the cost effectiveness of the method of notification.

We will always provide notice in accordance with any applicable law or industry code (such as the Customer Owned Banking Code of Practice).

How We Send Notices & Statements

We may send you notices and statements:

- by post, to the address recorded in our records or to a mailing address you nominate;
- by secure messaging via our internet banking platform;
- via the Mobile Banking App;
- by email to the address recorded in our records that you nominate;
- by advertisement on our website or
- by advertisement in the media, for some notices only.

If you agree, we may, instead of sending you a notice, post notices to our website for you to retrieve. We will tell you when information is available for you to retrieve, either at the time or on setting up a facility that will have regular postings to the website.

You can change your email address, or revert to receiving paper notices or statements, at any time.

Complaints

We have a dispute resolution system to deal with any complaints you may have in relation to your Account or Access Facility. Our dispute resolution policy requires us to deal with any complaint efficiently, speedily and sympathetically.

If you are not satisfied with the way in which we resolve your complaint, or if we do not respond speedily, you may refer the complaint to our external dispute resolution centre, being The Australian Financial Complaints Authority (**AFCA**). The contact details for AFCA are set out on page 19. Our staff must also advise you about our complaint handling process and the timetable for handling your complaint. We also have an easy to read guide to our dispute resolution system available on our website.

Complaints can be raised by contacting us as follows:

- Visiting your nearest branch;
- Calling 132 067;
- enquiries@regionalaustraliabank.com.au;
- Writing to us at:
  enquiries@regionalaustraliabank.com.au; or
  PO Box U631 University of New England NSW 2351.

Chequing

Chequing allows you to make payments by cheque. We will debit your Account for the value of cheques you draw.

Drawing a Cheque

If you cross a cheque, you are telling a financial institution that the cheque must be paid into an account with a financial institution and not cashed. Crossing a cheque means drawing two lines clearly across the face of the cheque.

'Not negotiable' and 'account payee only' cheques

The words 'not negotiable' between two parallel lines across the face of a cheque help to protect the true owner of a lost or stolen cheque. If you write 'account payee only' on a cheque you are directing the financial institution collecting the cheque to only pay the cheque into the account of the person named on the cheque. These words do not prevent the transfer of a cheque however may give you better protection against theft or fraud.

Deleting 'or bearer' on the cheque

Your pre-printed cheque forms have the words 'or bearer' after the space where you write the name of the person to whom you are paying the cheque. The cheque is a 'bearer' cheque.

If you cross out the words 'or bearer' and do not add the words 'or order', the cheque is still a bearer cheque. You can give yourself more protection against theft or fraud by crossing out the words 'or bearer' and adding the words 'or order'.

How do I stop payment on a cheque?

You can stop payment on a cheque by:

- Calling us and completing our stop payment form, or
- Writing to us with particulars to identify the cheque. You must, of course, do this before we have paid the cheque.

How do you reduce the risk of forgery?

When filling in a cheque:

- Start the name of the person to whom you are paying the cheque as close as possible to the word 'pay'
- Draw a line from the end of the person's name to the beginning of the printed words 'or bearer'
- Start the amount in words with a capital letter as close as possible to the words 'the sum of' and do not leave blank spaces large enough for any other words to be inserted. Also add the word 'only' after the amount in words
- Draw a line from the end of the amount in words to the printed '$'
- Start the amount in numbers close after the printed '$' and avoid any spaces between the numbers, and
- Always add a full stop '.' Or dash '-' to show where the dollars end and the cents begin and, if there are no cents, always write '.00' Or '-00' to prevent insertion of more numbers to the dollar figure.

When can we dishonour or not pay a cheque?

We can dishonour your cheque or not pay on it if:

- You have insufficient funds or available credit in your account to cover the cheque, However, we have discretion to allow the cheque to be paid and to overdraw your Account. If you overdraw your Account, we may charge you interest on the overdrawn amount or a daily fee for everyday your Account is overdrawn. Please refer to the section Overdrawing an Account;
- You have not drawn up the cheque clearly so we are unsure of what you want it to do;
- You have post-dated your cheque and it is presented for payment before the date on the cheque;
- The cheque is 'stale', that is, the date of the cheque is more than 15 months ago; or
- We have received notice of your death or mental incapacity.

We may not give you access to chequing if your banking history with Regional Australia Bank is not satisfactory or if you are under 18 years of age.

DIRECT DEBIT

One way you can authorise a participating biller to debit amounts from your eligible Account, as and when you owe those amounts to the biller, is a direct debit. The biller will provide you with a Direct Debit Request Service Agreement (**DDR Service Agreement**) for you to complete and sign to provide them with this authority.

To cancel the DDR Service Agreement, you can contact either the biller or us. If you contact us we will promptly stop the facility. We suggest that you also contact the biller.

If you believe a direct debit initiated by a biller is wrong you should contact the biller to resolve the issue. Alternatively, you may contact us. If you give us the information we require we will forward your claim to the biller. However, we are not liable to compensate you for your biller's error.

If you set up the payment on your Visa card, please contact us directly about unauthorised or irregular debits.

We can cancel your direct debit facility, in our absolute discretion, if 3 consecutive direct debit instructions are dishonoured. If we do this, billers will not be able to initiate a direct debit from your Account under their DDR Service Agreement. Under the terms of their DDR Service Agreement, the biller may charge you a fee for each dishonour of their direct debit request.

This section does not apply to PayTo, which provides an alternative method to pre-authorise a biller to debit amounts from your eligible account. For PayTo see Electronic Access Facilities & ePayments Conditions of Use Section 37 to Section 45.

PAYPAL

When you use PayPal you are authorising PayPal to debit amounts from your Account as a biller under direct debit. Please note that:

- you are responsible for all PayPal debits to your Account;
- if you dispute a PayPal debit, you can contact PayPal directly or ask us to do so;
- we are not responsible for compensating you for any disputed PayPal debit, or for reversing any disputed PayPal debit to your Account;
- if you want to cancel your DDR Service Agreement with PayPal, you can contact PayPal directly or ask us to do so;
- when you ask us to pass on a disputed transaction to PayPal, or your request to cancel your DDR Service Agreement with PayPal, we will do so as soon as practicable but we are not responsible if PayPal fails to respond as soon as possible or at all.

Other third party payment services may operate in a similar way to PayPal.

ELECTRONIC ACCESS FACILITIES & EPAYMENTS CONDITIONS OF USE

Section 1. INFORMATION ABOUT OUR EPAYMENTS FACILITIES

You should follow the guidelines in the box titled Important Information You need to Know Before Using a Device to Make Electronic Payments to protect against unauthorised use of your Visa card and pass code. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised epayments. Liability for such transactions will be determined in accordance with the ePayments Conditions of Use and the ePayments Code.

Important Information You Need to Know

- Sign the Access/Visa card as soon as you receive it.
- Familiarise yourself with your obligations to keep your Access/Visa card and pass codes secure.

- Familiarise yourself with the steps you have to take to report loss or theft of your Access/Visa card or to report unauthorised use of your Access/Visa card, BPAY®, Payto, phone or internet banking.
- Immediately report lost, theft or unauthorised use.
- If you change a pass code, do not select a pass code which represents your birth date or a recognisable part of your name.
- Do not store a user name and passcode for internet banking unprotected 'in a diary, computer or other personal electronic device'
- Never write the pass code on your Access/Visa card.
- Never write the pass code PIN on anything which is kept with or near your access/Visa card.
- Never lend your access/Visa card to anybody.
- Never tell or show your pass code to another person.
- Use care to prevent anyone seeing the pass code being entered on a device.
- Keep a record of the Visa card number and the Visa card hotline phone number for your area with your usual list of emergency phone numbers.
- Check your statements regularly for any unauthorised use.
- Immediately notify us when you change your address.
- ALWAYS access the phone banking or internet banking service only using the OFFICIAL phone numbers and URL addresses.
- If accessing internet banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history.
- ALWAYS REJECT any request to provide or to confirm details of your pass code. We will NEVER ask you to provide us with these details.

If you fail to ensure the security of your Visa card, access facility and pass codes you may increase your liability for unauthorised transaction.

Our epayments access facilities are:

Osko Payment	
Internet Banking	Visa Card
Phone Banking	BPAY®
payWave	Bank@Post
Mobile Banking App	PayTo

(**ePayment Access Facilities)**

You can access an Account using any of the ePayments Access Facilities applicable to the Account. Please refer to:

- the Summary of Accounts & Availability of Access Facilities brochure for the ePayments access facilities available for each Account type; and
- the Fees and Charges brochure for fees and charges in relation to ePayment Access Facilities.

The ePayments Conditions of Use govern all ePayments transactions made using any one of our ePayments Access Facilities.

VISA CARD

Our Visa Card allows you to make payments at any retailer displaying the Visa card logo, anywhere in the world. You can also withdraw cash from your Account, anywhere in the world, using an ATM displaying the ***Visa Card logo***. We will provide you with a PIN to use with your Visa Card.

Our Visa Card also allows you to:

- check your Account balances;
- withdraw cash from your Account;
- transfer money between Accounts
- deposit cash into your Account (at select ATMs only).

We may choose not to give you a Visa Card if your banking history with Regional Australia Bank is not satisfactory or if you are under 12 years of age.

You should follow the guidelines, below, to protect against unauthorised use of the Visa Card and PIN. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised ePayment Transactions. Liability for such transactions will be determined in accordance with section 20 of these Conditions of Use and the ePayments Code.

GUIDELINES FOR ENSURING THE SECURITY OF THE VISA CARD AND PIN

- Sign the Visa card as soon as you receive it;
- Keep the Visa card in a safe place;
- If you change the PIN, you must not select a PIN which represents your birth date or a recognisable part of your name;
- Never write the PIN on the Visa card;
- Never write the PIN on anything which is kept with or near the Visa card;
- Never lend the Visa card to anybody;
- Never tell or show the PIN to another person;
- Use care to prevent anyone seeing the Visa card number and PIN being entered at ePayments terminal;
- Immediately report the loss, theft or unauthorised use of the Visa card to Regional Australia Bank or to the Visa Card Hotline;
- Keep a record of the Visa card number and the Visa Card Hotline phone number for your area with your usual list of emergency phone numbers;
- Examine your periodical statement immediately upon receiving it to identify and report, as soon as possible, any instances where the Visa card has been used without your authority; and
- Immediately notify us of any change of address.

IMPORTANT INFORMATION ABOUT DISPUTES

If you believe a Visa Card transaction:

- was unauthorised;
- was for goods or services which did not match the description provided by the merchant or the merchant did not deliver them;

then you can ask us to 'dispute' the transaction, by reversing the payment to the merchant's financial

institution. However, we can only do a chargeback if you inform us of the disputed transaction within the timeframe determined by Visa. Currently the shortest cut-off time for notifying of chargeback circumstances is 30 days after the transaction, although longer periods may apply in particular circumstances. In some circumstances where the ePayments Code applies the time limits may not apply.

You are not able to reverse a transaction authenticated using Visa Secure unless we are liable as provided in the ePayments Conditions of Use.

You should inform us as soon as possible if you become aware of circumstances which might entitle you to a dispute and let us have the cardholder's copy of the Visa transaction receipt in question.

DIGITAL WALLET (APPLE PAY, GOOGLE PAY ETC)

If you wish to use your Visa debit card, including any multi-network debit card that also uses eftpos, or your Visa credit card (**Card**) in a digital wallet, such as Apple Pay or Google Pay, please contact us to see if your Card is compatible. If your Card is not compatible, we will arrange for you to be issued with a compatible Card.

The use and functioning of a digital wallet is governed by the conditions of use for the app or your telecommunications provider that you are using. We recommend that you read these conditions of use carefully before using the digital wallet.

We are not the provider of the digital wallet and are not responsible for its use and function. You should contact the digital wallet provider's customer service if you have questions concerning how to use the digital wallet or problems with the digital wallet.

When you load your Card into a digital wallet, you acknowledge and agree that we may collect, use and disclose your personal information and card or transaction information between us, the digital wallet provider, your card provider, relevant card schemes, including Visa and eftpos and, where applicable, EFTPOS Payments Australia Limited (EPAL), token service providers and other service providers involved in identification and verification, tokenisation, provisioning, lifecycle management, payment processing, fraud management, dispute handling and security, for the purpose of registering your Card, enabling and administering the digital wallet service, facilitating purchases or other transactions you initiate using your Card registered in a digital wallet, and complying with legal, regulatory and scheme Requirements. You authorise use to provide that information for those purposes. We are not responsible for any loss, injury or other harm you suffer in connection with the digital wallet provider's use of your information.

The registration of your Card into a digital wallet is subject to us identifying and verifying you, which will be at our discretion.

We do not make any guarantees that the digital wallet will be accepted at all merchants.

We are not liable for any loss, injury or inconvenience you suffer as a result of a merchant refusing to accept the digital wallet.

These terms apply to the use by you of your Card in a digital wallet. By registering your Card in a digital wallet you agree to these terms.

You must not use or distribute any software, software development kit, technical information or documentation made available to you in connection with the digital wallet service, except to the extent reasonably necessary to enable payment transmission and payment processing using your Card through the digital wallet.

Where your Card is a multi-network debit card, the digital wallet service may support tokenisation and related processing for both Visa and eftpos.

We are not responsible if there is a security breach affecting any information stored in the digital wallet or sent from the digital wallet. This is the responsibility of the digital wallet provider.

There are no transaction fees for using your Card in a digital wallet. However, there may be charges from your telecommunications provider.

Important Information You Need to Know Before Using Your Digital Wallet on a Mobile Phone

You must protect and keep confidential your User ID, phone lock, passcode, passwords, and all other information required for you to make purchases with your Card using a digital wallet.

Always protect your device passcodes by using a unique number or a pattern that is not obvious or can be easily guessed. Take precautions when using your digital wallet. Try to memorise your passcode or carefully disguise it. Never keep a record of your passcode with your device, on your device or computer, or tell anyone your passcode.

Any person who can unlock the device your digital wallet is stored on may be able to make transactions using your Card stored in your digital wallet.

You are responsible for ensuring that:

- only your biometric identifier (being your finger print, faceprint or similar biometric identifier) is registered on the device;
- that the digital wallet is not shared with anyone and is only used by you;
- ensure that your device passcode is kept secure in the same way as you would your internet banking password or PIN;
- that your device is kept safe and secure (including by locking it when not in use or when it is unattended and by installing up to date anti-virus software on it); and
- that your Visa Card is removed from your device before disposal.

If you:

- allow another person's biometric identifier to be registered on your device; or
- share your device passcode;

you are taken to have authorised that person to transact on your Account using your Card stored in your digital wallet.

This could result in significant loss or liability

in relation to such transactions.

You are required to notify us immediately:

- if your device is lost or stolen;
- if you believe that your security credentials have been compromised;
- if you suspect any fraud associated with your digital wallet.

Once notified, we will then suspend the use of your Card. This helps us protect you for addition loss or liability.

You may become liable for any unauthorised transactions if you unreasonably delay notifying us.

We may block, suspend or terminate your Visa Card used in your digital wallet:

- if we suspect your Card is being used fraudulently;
- you are in breach of these Conditions of Use;
- if we are required to under any applicable law;
- if we are directed to by a digital wallet provider;
- for any reason we consider reasonable.

We may cease supporting the use of any of our cards in a digital wallet at any time.

We are not liable for any loss arising from your use of a digital wallet to the extent the loss was caused:

- by your fraud; and/or
- your use of the digital wallet in a manner not permitted by the provider or these Conditions of Use.

You may remove your Card from the digital wallet provider by following the digital wallet providers procedures for removal.

If you add your Card to one of your devices and have other devices sharing the same account (**Other Devices**), this may permit the users of the Other Devices to see your Card information. Please contact your digital wallet provider for more information.

We may vary or amend the clauses relating to the use of your Card in a digital wallet and you agree to such amendments by continuing to use your Card in the digital wallet.

BANK@POST®

Bank@Post is Australia Post's agency banking service, with facilities at over 3,200 Australia Post outlets around the nation.

To make deposits to and withdrawals from your Account, all you need is a Regional Australia Bank Visa Card which you can use with an accompanying PIN.

PHONE BANKING, INTERNET BANKING AND MOBILE BANKING APP

Phone banking, internet banking and the Mobile Banking App gives you remote access to your Account that allows you to obtain information about your Account, to transfer money between Accounts, to make BPAY® payments and to transfer money to Accounts at other financial institutions.

Section 2. DEFINITIONS

In these ePayments Conditions of Use:

"Account" means your Account with us;

"Account Details" means our record of your account, including BSB, account number, account name, your full legal name, any other name you prefer us to use and account activity.

"Account Owner" means a Member or a Customer Regional Australia Bank.. The Account owner is the person responsible for all transactions on the Account.

"access method" means a method we authorise for you to use as evidence of your authority to make an ePayments transaction or to access information about your Account, that does not require a manual signature, and includes, but is not limited to:

- in the case of phone banking, internet banking or the Mobile Banking App, any combination of your Visa Card and PIN, your membership or customer number, secret code, password, pattern and PIN;
- in the case of BPAY® - any combination of your Visa Card and PIN, your Account number, secret code or password;
- in the case of Visa Card - your Visa Card and PIN used at an ePayments terminal;

"additional cardholder" means a person or entity other than the account owner who has been nominated by an account owner to operate the account by use of a Visa card.

"ATM" means automatic teller machine;

"authorised user" means you and any person you have considered to operate your Account;

"BECS Procedures" means the Bulk Electronic Clearing System Procedures as existing from time to time;

"BPAY®" means the electronic payment scheme called BPAY® operated in co-operation between Australian financial institutions, which enables you to effect bill payments to billers who participate in BPAY®, either via phone or internet access or any other access method as approved by us from time to time;

"business day" means any day on which we are open for business;

"Click to Pay" is a secure online checkout experience that enables you to transact at participating merchants without manually entering your Visa Card details.

"Closed" in relation to a PayID, means a PayID which is removed from the PayID service, and unable to be used for NPP Payments;

"Customer" means a person or entity that has been approved to be a customer in accordance with the Regional Australia Bank Constitution.

"device" means a device we give to a user that is used to perform a transaction. Examples include:

(a) Visa Card; and

(b) token issued by a subscriber that generates a pass code.

"EFTPOS" means electronic funds transfer at the point of sale—a network for facilitating transactions at point of sale;

"direct debit" means a "Direct Debit Request" as defined in the BECS Procedures;

"facility" means an arrangement through which you can perform transactions;

"**Financial abuse"** means conduct that controls, exploits, sabotages, or coerces a person's access to or use of money or financial services, including through patterns of intimidation or control.

"identifier" means information that a user:

(a) knows but is not required to keep secret, and

(b) must provide to perform a transaction;

Examples include a member number or customer number.

"ePayments terminal" means the electronic equipment, electronic system, communications system or software that we, our agents or any third party control or provide for use with a Visa Card and PIN to conduct an ePayments transaction, for example, an automatic teller machine (ATM) or point of sale terminal (EFTPOS);

"ePayments transaction" means an electronic funds transfer to or from your Account using an access method and includes transactions carried out by means of:

- Visa Card
- BPAY®
- Osko® Payment
- Internet Banking
- Phone Banking
- Mobile device App

"internet banking" means a service we provide from time to time through our internet site which enables you to electronically receive information from us about, or to give us instructions concerning, your Accounts which we then act on;

"internet site" means our site at:

regionalaustraliabank.com.au

"Locked" in relation to a PayID, means a PayID which we have temporarily disabled in the PayID service;

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

"Member" means a person or entity approved for membership and issued a member share in accordance with the Regional Australia Bank Constitution.

"Migrated DDR Mandates" has the meaning given in Section 42.1;

"Misdirected Payment" means a payment erroneously credited to the wrong Account because of an error in relation to the recording of the associated Account information in the BPay or PayID service;

"Mistaken Payment" means a payment, made by a payer who is a 'user' for the purposes of the ePayments Code, which is erroneously credited to the wrong Account because of the payer's error;

"Mobile Banking App" means a tool we provide from time to time that is downloaded to a mobile device from the Apple® App Store ® or the Google® Play Store®;

"NPP" means the New Payments Platform operated by NPP Australia Limited (ACN 601 428 737).

"NPP Payments" means payments cleared and settled via the NPP;

"Online Banking Services" is the term used to encompass phone banking, internet banking, mobile banking and the Mobile Banking App;

"Organisation ID" means an identifier for a customer that is a business customer or organisation, constructed by us as [business name] and/or [description of business/campaign/product] and/or [geographic location/state]

"Osko" leverages PayID to make payment via an easy to remember identifier.

"pass code" means a password or code that the user must keep secret, that may be required to authenticate a transaction or user. A pass code may consist of numbers, letters, a combination of both, a phrase or a swipe pattern. Examples include:

- personal identification number (PIN),
- internet banking password,
- phone banking password,
- code generated by a virtual or physical security token,
- Osko Payments smart address (Pay ID),
- lock mode for the Mobile Banking App, being a PIN or pattern,
- A pass code does not include a number printed on a device (e.g. a security number printed on a credit or debit card).

"participating online merchant means a retailer or merchant who offers goods or services for sale online, who is a participant in Visa Secure

"PayID" means the identifier you choose to use to receive NPP Payments;

"PayID Name" means the name we give you or the name selected by you (with our approval) to identify you to Payers when your PayID is used to make an NPP Payment;

"PayID Type" means the type of identifier you select for receiving NPP Payments, which may be your phone number, mobile number, email address, Australian company number, Australian business number or Organisation ID;

"regular payment arrangement" means either a recurring or an instalment payment agreement between you (the cardholder) and a Merchant in which you have preauthorised the Merchant to bill your Account at predetermined intervals (eg. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction.

"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 account. Other than in Section 37 "Creating a PayTo Payment Agreement", it includes a Migrated DDR Mandate;

"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 account;

"PayTo" means the service which enables us to process NPP Payments from your 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;

"phone banking" means a service we offer from time to time through a phone communication network which enables you to electronically receive information from us about, or to give us instructions concerning, your Accounts which we then act on;

"transaction" means a transaction to which these ePayment Conditions of Use apply;

"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 transaction" means a transaction that is not authorised by a user

"user" means you or an individual you have authorised to perform transactions on your Account, including:

- a third party signatory to your Account; and
- a person you using an additional card;

"Visa Secure" means the online transaction authentication service provided by us (or our nominated service provider).

"Visa Card" means the Visa debit or credit card issued by us to you or an additional cardholder.

"**we**", "**us**" or "**our**" means Regional Australia Bank;

"**you**" means:

- the person, persons or entity in whose name the Regional Australia Bank Account and Access Facility is held;
- any third party you nominate to operate on the Regional Australia Bank Account and Access Facility; and
- any person you authorise us to issue a Visa Card to.

Section 3. TRANSACTIONS

1. The ePayment Conditions of Use apply to payment, funds transfer and cash withdrawal transactions that are:
   (c) initiated using electronic equipment; and
   (d) not intended to be authenticated by comparing a manual signature with a specimen signature.
2. The ePayment Conditions of Use apply to the following transactions:
   (i) electronic card transactions, including ATM, EFTPOS, credit card and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature;
   (ii) phone banking and bill payment transactions;
   (iii) internet banking transactions, including 'Pay Anyone';
   (iv) online transactions performed using a card number and expiry date;
   (v) online bill payments (including BPAY);
   (vi) direct debits;
   (vii) transactions using electronic devices (including smart phones and watches); and
   (viii) PayTo Payments; and
   (ix) Osko Payments.

Section 4. HOW TO REPORT LOSS, THEFT OR UNAUTHORISED USE OF YOUR CARD OR PASS CODE

1. If you believe your Visa Card has been misused, lost or stolen or the PIN has become known to someone else, you must immediately contact us during business hours or visit our website for the up to date details on reporting numbers. You can also block access to your Visa Card via the Mobile Banking App.
2. If you believe your token has been misused, lost or stolen you must immediately contact us during business hours.
3. You must provide the following information when notifying us or the Visa card hotline:
   - the Visa Card number;
   - the name of your institution being Regional Australia Bank; and
   - any other personal information you are asked to provide to assist in identifying you and the Visa card.
4. You will be provided a reference number verifying the date and time of your notification. Please retain this reference number.

(i) If you have contacted the Visa Card Hotline please contact us during business hours to confirm the loss or theft.

5. If the Visa Card Hotline is not operating when you attempt notification, you must report the loss, theft or unauthorised use to us as soon as possible during business hours. We will be liable for any losses arising because the Visa Card Hotline is not operating at the time of attempted notification, provided you report the loss, theft or unauthorised use to us as soon as possible during business hours.
6. If the loss, theft or misuse, occurs outside Australia you must notify an organisation displaying the VISA sign and also then confirm the loss, theft or misuse of the card:
   (i) with us by phone; or
   (ii) by telephoning the Visa Card Hotline.

Section 5. HOW TO REPORT UNAUTHORISED USE OF ONLINE BANKING SERVICES

1. If you believe that your access method, or any part of your access method, has been misused, lost or stolen, or, where relevant, your access details, be they your pass code, password or PIN, has become known to someone else, you must contact us immediately.
2. If you believe an unauthorised transaction has been made and your access method uses a pass code, biometrics, password or PIN you should change that pass code immediately.

Section 6. EPAYMENTS TRANSACTION LIMITS

1. We limit the amount of ePayments transactions you may make on any one day or other period, either generally or in relation to a particular access method. These transaction limits are set out in the Fees and Charges brochure.
2. We may also require you to apply for new transaction limits if you change any passcode, in

an access method. We will require you to provide proof of identity that satisfies us. We may reduce transaction limits for security reasons.

Section 7. Processing ePayments Transactions

1. We will debit the value of all withdrawal ePayments transactions and credit the value of all deposit ePayments transactions to or from your Account in accordance with your instructions when the appropriate access method is used.
2. If you close your Account before an ePayments transaction debit is processed, you will remain liable for any dishonour fees incurred in respect of that transaction.
3. Transactions will not necessarily be processed to your Account on the same day.

Section 8. Using Online Banking Services

1. We will tell you from time to time:
   - what services are available using phone banking, internet banking or the Mobile Banking App;
   - which of your Accounts you can access using phone banking, internet banking or the Mobile Banking App.
2. We cannot effect your phone banking, internet banking or the Mobile Banking App instructions if you do not give us all the specified information or if you give us inaccurate information.
3. If you instruct us to make more than one payment from your Account, we will determine the order of making the payments.
4. We do not warrant that:
   - the information available to you about your Accounts through our online banking services is always up to date;
   - you will have 24 hour a day, 7 days per week, access to phone banking, internet banking or the Mobile Banking App.
   - data you transmit via phone banking, internet banking or the Mobile Banking App is totally secure.
5. After you have finished accessing your Account using:
   - phone banking, you must ensure that you end the phone call to our phone banking service;
   - internet banking, you must ensure that you log off from our internet banking service; and
   - the Mobile Banking App, you must ensure that you log off from the Mobile Banking App.
6. We may require additional authentication methods to be used for phone banking, internet banking and the Mobile Banking App. These methods are used to provide additional security to your Account and funds. In the event that you refuse additional authentication methods, we may restrict the functionality and availability of internet and mobile banking.
7. Periodical payments will retry for 7 business days, including Saturdays, if rejected. Periodical payments that have been rejected after 7 business days will be cancelled. Cancellation will occur for each of the Periodical Payment transaction types, transfers, loan repayments and cheque withdrawals.

Section 9. Mistaken Internet Payments

1. In this section:
   (a) **"direct entry**" means a direct debit or direct credit;
   (b) **"mistaken internet payment"** means a payment by a user through a 'Pay Anyone' banking facility and processed by an ADI where funds are paid into the Account of an unintended recipient because the user enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:
   (c) the user's error, or
   (d) the user being advised of the wrong BSB number and/or identifier.

   This does not include payments made using BPay or PayTo.
   (a) **"receiving ADI"** means an ADI whose customer has received an internet payment;
   (b) **"unintended recipient"** means the recipient of funds as a result of a mistaken internet payment;
2. When you report a mistaken internet payment, we must investigate whether a mistaken internet payment has occurred.
3. If we are satisfied that a mistaken internet payment has occurred, we must send the receiving ADI a request for the return of the funds.

   Note: Under the ePayments Code, the receiving ADI must within 5 business days:
   (a) acknowledge the request by the sending ADI for the return of funds, and
   (b) advise the sending ADI whether there are sufficient funds in the Account of the unintended recipient to cover the mistaken internet payment.
4. If we are not satisfied that a mistaken internet payment has occurred, we will not take any further action.
5. We must inform you of the outcome of the reported mistaken internet payment in writing and within 30 business days of the day on which the report is made.
6. You may complain to us (see Page 4 Complaints) about how the report is dealt with, including that we and/or the receiving ADI:
   (i) are not satisfied that a mistaken internet payment has occurred;
   (ii) have not complied with the processes and timeframes set out in clauses -Section 1.5, or as described in the box below.
7. When we receive a complaint we must:
   (i) deal with the complaint under our internal dispute resolution procedures
   (ii) not require you to complain to the receiving ADI.
8. If you are not satisfied with the outcome of a complaint, you are able to complain to our external dispute resolution scheme provider.

Note: If we are unable to return funds to you because the unintended recipient of a mistaken internet payment does not cooperate, you can complain to our external dispute resolution scheme provider.

Information about a receiving ADI's obligations after we request return of funds

The information set out in this box is to explain the process for retrieving mistaken payments under the ePayments Code, setting out what the processes are, and what you are entitled to do.

This information does not give you any contractual entitlement to recover the mistaken payment from us or to recover the mistaken payment from the receiving ADI.

Process where funds are available & report is made within 10 business days

- If satisfied that a mistaken internet payment has occurred, the receiving ADI must return the funds to the sending ADI, within 5 business days of receiving the request from the sending ADI if practicable or such longer period as is reasonably necessary, up to a maximum of 10 business days.
- If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder.
- The sending ADI must return the funds to the holder as soon as practicable.

Process where funds are available & report is made between 10 business days & 7 months

- The receiving ADI must complete its investigation into the reported mistaken payment within 10 business days of receiving the request.
- If satisfied that a mistaken internet payment has occurred, the receiving ADI must:
  a. prevent the unintended recipient from withdrawing the funds for 10 further business days, and
  b. notify the unintended recipient that it will withdraw the funds from their Account, if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds.
- If the unintended recipient does not, within 10 business days, establish that they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days after the expiry of the 10 business day period, during which the unintended recipient is prevented from withdrawing the funds from their Account.
- If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to the holder.
- The sending ADI must return the funds to the holder as soon as practicable.

Process where funds are available and report is made after 7 months

- If the receiving ADI is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds to the user.
- If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder.
- If the unintended recipient consents to the return of the funds:
  a. the receiving ADI must return the funds to the sending ADI, and
  b. the sending ADI must return the funds to the holder as soon as practicable.

Process where funds are not available

- Where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient credit funds available in the Account of the unintended recipient to the full value of the mistaken internet payment, the receiving ADI must use reasonable endeavours to retrieve the funds from the unintended recipient for return to the holder (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

Section 10. USING BPAY®

BPAY®

BPAY® allows you to pay bills bearing the BPAY® logo, through either phone banking, internet banking or the Mobile Banking App.

1. You can use BPAY® to pay bills bearing the BPAY® logo from those Accounts that have the BPAY® facility.
2. When you tell us to make a BPAY® payment you must tell us the biller's code number (found on your bill), your Customer Reference Number (eg. your Account number with the biller), the amount to be paid and the Account from which the amount is to be paid.
3. We cannot effect your BPAY® instructions if you do not give us all the specified information or if you give us inaccurate information.
4. 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.

Section 11. PROCESSING BPAY® PAYMENTS

1. We will attempt to make sure that your BPAY® payments are processed promptly by participants in BPAY®, and you must tell us promptly if:
   - you become aware of any delays or mistakes in processing your BPAY® payment;
   - you did not authorise a BPAY® payment that has been made from your Account; or
   - you think that you have been fraudulently induced to make a BPAY® payment.

   Note: Please keep a record of the BPAY® receipt numbers on the relevant bills.
2. A BPAY® payment instruction is irrevocable.
3. Except for future-dated payments you cannot stop a BPAY® payment once you have instructed us to make it and we cannot reverse it.
4. We will treat your BPAY® payment instruction as valid if, when you give it to us, you use the correct access method.
5. You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay - for these errors see Section 11.9) when making a BPAY® payment or if you did not authorise a BPAY® payment that has been made from your Account.

   Note: You must provide us with written consent addressed to the biller who received that 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.
6. A BPAY® payment is treated as received by the biller to whom it is directed:
   - on the date you direct us to make it, if we receive your direction by the cut off time on a banking business day, that is, a day in Sydney or Melbourne when banks can effect settlements through the Reserve Bank of Australia; and
   - otherwise, on the next banking business day after you direct us to make it.

   Note: BPAY® payment may take longer to be credited to a biller if you tell us to make it on a Saturday, Sunday or a public holiday or if another participant in BPAY® does not process a BPAY® payment as soon as they receive its details.
7. A delay may occur processing a BPAY® payment if:
   - there is a public or bank holiday on the day after you instruct us to make the BPAY® payment;
   - you tell us to make a BPAY® payment on a day which is not a banking business day or after the cut off time on a banking business day; or
   - a biller, or another financial institution participating in BPAY®, does not comply with its BPAY® obligations.
8. If we are advised that your payment cannot be processed by a biller, we will:
   - advise you of this;
   - credit your Account with the amount of the BPAY® payment; and
   - take all reasonable steps to assist you in making the BPAY® payment as quickly as possible.
9. You must be careful to ensure you tell us the correct amount you wish to pay. If you make a BPAY® payment and later discover that:
   - the amount you paid was greater than the amount you needed to pay - you must contact the biller to obtain a refund of the excess; or
   - the amount you paid was less than the amount you needed to pay - you can make another BPAY® payment for the difference between the amount you actually paid and the amount you needed to pay.
10. If you are responsible for a mistaken BPAY® payment and we cannot recover the amount from the person who received it within 20 business days of us attempting to do so, you will be liable for that payment.

Section 12. FUTURE-DATED BPAY® PAYMENTS

You may arrange BPAY® payments in advance of the time for payment. If you use this option you should be aware of the following:

1. You are responsible for maintaining, in the Account to be drawn on, sufficient cleared funds to cover all future-dated BPAY® payments (and any other drawings) on the day(s) you have nominated for payment or, if the Account is a credit facility, there must be sufficient available credit for that purpose.
2. If there are insufficient cleared funds or, as relevant, insufficient available credit, the BPAY® payment will not be made and you may be charged a dishonour fee. Please refer to our Fees and Charges brochure.
3. You are responsible for checking your Account transaction details or Account statement to ensure the future-dated payment is made correctly.
4. You should contact us if there are any problems with your future-dated payment.
5. You must contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the BPAY® payment on or after that date.

Section 13. CONSEQUENTIAL DAMAGE FOR BPAY® PAYMENTS

1. This clause does not apply to the extent that it is inconsistent with or contrary to any applicable law or code of practice to which we have subscribed. If those laws would make this clause illegal, void or unenforceable or impose an obligation or liability which is prohibited by those laws or that code, this clause is to be read as if it were varied to the extent necessary to comply with those laws or that code or, if necessary, omitted.
2. We are not liable for any consequential loss or damage you suffer as a result of using BPAY® or Osko® other than loss due to our negligence or in relation to any breach of a condition or warranty implied by the law of contracts for the supply of

goods and services which may not be excluded, restricted or modified at all, or only to a limited extent.

Section 14. USING A VISA CARD

1. You agree to sign your Visa Card immediately upon receiving it and before using it as a means of preventing fraudulent or unauthorised use of the Visa Card. You must ensure that any other cardholder you authorise also signs their Visa Card immediately upon receiving it and before using it.
2. We will advise you from time to time:
   - what ePayments transactions may be performed using the Visa Card;
   - what ePayments terminals of other financial institutions may be used; and
   - what the daily cash withdrawal limits are.
3. Please refer to the Fees and Charges brochure for details of current transaction limits. Section 6 that sets out how we can vary daily withdrawal limits from time to time.
4. You may only use your Visa Card to perform transactions on those Accounts we permit. We will advise you of the Accounts which you may use your Visa Card to access.
5. The Visa Card always remains our property.

Section 15. USING A VISA CARD OUTSIDE AUSTRALIA

1. You agree to reimburse us for any costs, fees or charges of any nature arising out of a failure to comply with any exchange control requirements.
2. All transactions made overseas on your Visa Card will be converted into Australian currency by VISA Worldwide, and calculated at a wholesale market rate selected by VISA from within a range of wholesale rates or the government mandated rate that is in effect one day prior to the Central Processing Date (that is, the date on which VISA processes the transaction).
3. All transactions made overseas on your Visa Card are subject to a conversion fee. Please refer to the Fees and Charges brochure for the current conversion fee.
4. Some overseas merchants and ePayments terminals charge a surcharge for making an ePayments transaction using your Visa Card. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price.
5. The VISA hotline number is available on our website.

Section 16. ADDITIONAL VISA CARD

1. You may authorise us, if we agree, to issue an additional Visa Card to an additional cardholder provided if the card is issued to an individual that they are over the age of 12.
2. Not all additional Visa Card's will allow withdrawals, we will notify you and the additional card holder at the time of issuing the Visa Card if this is the case.
3. You will be liable for all transactions carried out on the additional Visa Card linked to Your Account.
4. We will issue a separate passcode to each additional Visa Card.
5. You must ensure that the additional Visa Card and associated passcode are used in accordance with these Conditions of Use.
6. To cancel the additional Visa Card you must call us on 132 067.
7. You may not be liable for the continued use of the additional Visa Card from the date that you have notified us that you want it cancelled.

Section 17. USING VISA CARD TO MAKE DEPOSITS AT EPAYMENT TERMINALS

1. This Section only applies to deposits made at ePayments terminals using your Visa Card.
2. Any deposit you make at an ePayment Terminal will not be available for you to draw against until your deposit has been verified by the ePayment Terminal and accepted by us.
3. Cheques will not be available to draw against until cleared.
4. Your deposit is accepted once we have certified it in the following way:
   (a) your deposit envelope will be opened in the presence of any two persons we authorise;
   (b) should the amount you record differ from the amount counted in the envelope, we may correct your record to the amount counted;
   (c) our count is conclusive in the absence of manifest error or fraud;
   (d) we will notify you of any correction.
5. If the amount recorded by the ePayment Terminal as having been deposited should differ from the amount counted in the envelope by us, we will notify you of the difference as soon as possible and will advise you of the actual amount which has been credited to your Account.
6. We are responsible for the security of your deposit after you have completed the transaction at the ePayment Terminal (subject to our verification of the amount you deposit).

Section 18. USE AFTER CANCELLATION OR EXPIRY OF THE VISA CARD

1. You must not use your Visa Card:
   (a) before the valid date or after the expiration date shown on the face of the Visa Card; or
   (b) after the Visa Card has been cancelled.
2. You will continue to be liable to reimburse us for any indebtedness incurred through such use whether or not you have closed your Account.

Section 19. EXCLUSIONS OF VISA CARD WARRANTIES AND REPRESENTATIONS

1. We do not warrant that merchants, ePayments terminals or ATMs displaying Visa Card signs or promotional material will accept the Visa Card.
2. We do not accept any responsibility should a merchant, bank or other institution displaying Visa Card signs or promotional material, refuse to accept or honour the Visa Card.
3. We are not responsible for any defects in the goods and services you acquire through the use of the Visa Card. You acknowledge and accept that all complaints about these goods and services must

be addressed to the supplier or merchant of those goods and services.

Section 20. Your Liability For ePayments Transactions

1. You are liable for all losses caused by an unauthorised ePayments transaction unless any of the circumstances specified in this Section apply.
2. You are not liable for losses caused by unauthorised ePayments transactions:
   (a) where it is clear that you have not contributed to the loss; and
   (b) that are caused by the fraudulent or negligent conduct of employees or agents of:
   - us;
   - any organisation involved in the provision of the ePayments system or BPAY®;
   - in the case of Visa Card - any merchant; or
   - in the case of BPAY® - any biller;

   (a) relating to a forged, faulty, expired or cancelled access method or any part of the access method;
   (b) that are caused by the same ePayments transaction being incorrectly debited more than once to the same Account;
   (c) resulting from unauthorised use of your access method or any part of your access method:
   - before you receive all parts of your access method necessary for that unauthorised ePayments transaction; or
   - after you notify us in accordance with Section 4 or Section 5 that your access method or any part of your access method has been misused, lost or stolen or used without your authorisation, or, where relevant, that the security of your pass code has been breached.
3. You will be liable for any loss of funds arising from unauthorised ePayments transactions if the loss occurs before you notify us that your access method or any part of your access method has been misused, lost or stolen or used without your authorisation, or, where relevant, the pass code has become known to someone else, and if we prove, on the balance of probabilities, that you contributed to the loss through:
   (a) your fraud or, where relevant, your failure to keep the pass code secure in accordance with Section 1; or
   (b) unreasonably delaying in notifying us of the misuse, loss, theft or unauthorised use of the access method or any part of your access method or, where relevant, of the pass code becoming known to someone else, and the loss occurs between the time you did, or reasonably should have, become aware of these matters and the time of notification to us.

   However, you will not be liable for:
   (a) the portion of the loss that exceeds any applicable daily or periodic transaction limits;
   (b) the portion of the loss on your Account which exceeds the balance of your Account (including any prearranged credit); or
   (c) all losses incurred on any Account which you had not agreed with us could be accessed using the access method.
4. Where a pass code is required to perform the unauthorised ePayments transaction and Section 20(3) does not apply, your liability for any loss of funds arising from an unauthorised ePayments transaction, if the loss occurs before you notify us that your access method or any part of your access method has been misused, lost, stolen or used without your authorisation, is the lesser of:
   (a) $150;
   (b) the balance of your Account, including any prearranged credit; or
   (c) the actual loss at the time you notify us that your access method or any part of your access method has been misused, lost, stolen or used without your authorisation, or, where relevant, of the pass 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 your Account).
5. In the case of BPAY®, if you notify us that a BPAY® payment made from your Account is unauthorised, you must provide us with a written consent addressed to the biller who received that BPAY® payment allowing us to obtain information about your Account with that biller as is reasonably required to investigate the 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.
6. Notwithstanding any of the above provisions your liability will not exceed your liability under the ePayments Code, where the code applies.
7. If, in cases not involving ePayments Transactions, the Visa Card or PIN are used without authority, you are liable for that use before notification to Regional Australia Bank or the Visa Card Hotline of the unauthorised use, up to your current daily withdrawal limit.

Section 21. Malfunction

1. You will not be responsible for any loss you suffer because the home banking system, BPAY®, or an ePayments terminal accepted your instructions but failed to complete a transaction.
1. In the event that there is a breakdown or interruption to our home banking system or any BPAY® system, or malfunction to an ePayments terminal, and you should have been aware that it was unavailable for use or malfunctioning, we will only be responsible for correcting errors in your Account and refunding any fees or charges imposed on you as a result.

Section 22. CANCELLATION OF VISA CARD OR OF ACCESS TO ONLINE BANKING SERVICES, BPAY® OR PAYTO

1. You may cancel your Visa Card, your access to phone banking, internet banking, the Mobile Banking App, BPAY®, Osko® or PayTo at any time by contacting us.
2. We may immediately cancel or suspend your Visa Card or your access to phone banking, internet banking (including the Mobile Banking App), BPAY® or Osko® at any time:
   (a) for security reasons
   (b) if you breach these ePayments Conditions of Use;
   (c) you, or someone acting on your behalf, is being fraudulent;
   (d) in the case of Osko, we suspect that you are using Osko in a manner that is likely to affect out ability to continue providing Osko to you or our other customers;
   (e) in the case of Osko or PayTo, if we cease to be a participant in Osko pr PayTo;
   (f) for any other reason set out in CLOSING ACCOUNTS, CANCELLING ACCESS FACILITIES & DELAYING, BLOCKING, FREEZING OR REFUSING TRANSACTIONS on page 5.

   In the case of Visa Card, we may cancel the Visa Card by capture of the Visa Card at any ePayments terminal.
3. We may cancel your Visa Card or your access to phone banking, internet banking (including the Mobile Banking App), BPAY® Osko or PayTo for any reason by giving you 30 days notice. The notice does not have to specify the reasons for cancellation.
4. In the case of Visa Card, you will be liable for any transactions you make using your Visa Card before the Visa Card is cancelled but which are not posted to your Account until after cancellation of the Visa Card.
5. In the case of phone banking, internet banking (including the Mobile Banking App), BPAY® Osko or PayTo if, despite the cancellation of your access to phone banking, internet banking (including the Mobile Banking App), BPAY® Osko or PayTo you carry out a transaction using the relevant access method, you will remain liable for that transaction.
6. Your Visa Card or your access to phone banking, internet banking (including the Mobile Banking App), BPAY® Osko or PayTo will be terminated when:
   (a) we notify you that we have cancelled your Visa Card or your access method to the Account with us;
   (b) you close the last of your Accounts with us to which the Visa Card applies or which has phone banking, internet banking (including the Mobile Banking App), BPAY® Osko or PayTo access;
   (c) you cease to be our Member or Customer; or
   (d) you alter the authorities governing the use of your Account or Accounts to which the Visa Card applies or which has phone banking, internet banking (including the Mobile Banking App), BPAY® Osko or PayTo access (unless we agree otherwise).
7. In the case of Visa Card, we may demand the return or destruction of any cancelled Visa Card.

Section 23. VISA SECURE

1. You may use Visa Secure to make purchases online. However, the Visa Secure Service may only be available in connection with participating online merchants.
2. When making an online purchase or other transaction for which Visa Secure applies, you may be asked to provide certain information to us that allows us to validate your identity and verify that you are the cardholder of the specified Visa card, such information includes, but is not limited to, a One Time Password. The information that you provide may be validated against information we hold about you and may be validated against information held by third parties.
3. If you are unable to provide the requested information to validate your identity, or if the information you provide is inaccurate or incomplete, or if the authentication process otherwise fails, the merchant may not accept your Visa card or payment for that transaction, and you may be unable to complete an online transaction using your Visa card.
4. In order to use Visa Secure, you must have the equipment and software necessary to make a connection to the Internet.
5. In the event you have a question regarding the authentication process or a transaction using your Visa card, you should contact us.

Section 24. ADDITIONAL CARDHOLDERS AND VISA SECURE

1. Subject to the account terms and conditions, you will be liable for all transactions conducted on your account which are undertaken by an additional cardholder.
2. Additional cardholders may use the Visa Secure service, but may be required to confirm their identity using the primary account holders' details.

Section 25. TERMINATION OF VISA SECURE

1. We may discontinue, terminate or suspend (permanently or temporarily) the Visa Secure service, or any part of the Visa Secure service, without giving you prior notice. We may also change any aspect or functionality of the Visa Secure service at any time without giving you prior notice.

Section 26. PARTICIPATING ONLINE MERCHANT

1. You will know that an online merchant is a participating online merchant because you will see the Visa Secure logo and you may be asked to verify your identity before completing an online transaction with that merchant.
2. We do not endorse or recommend in any way any participating online merchant.

3. Your correspondence or business dealings with, or participation in promotions of, online stores through Visa Secure, including payment for and delivery of related goods or services not purchased via Visa Secure, and any other terms, conditions, warranties or representations associated with such dealings, are solely between you and the online store. Except as otherwise required by law, we have no responsibility or liability whatsoever arising out of or related to those dealings or the online store's goods, services, acts or omissions.

Section 27. Exclusion of Liabilities and visa secure

1. Subject to any warranty which is imported into these Conditions of Use by law and which cannot be excluded, the Visa Secure service is provided by us "as is" without warranty of any kind, either express or implied, including, but not limited to, any implied warranties of merchantability, fitness for a particular purpose, title or non-infringement.
2. We will not be liable for any damages whatsoever arising out of or in relation to:
   (a) your use of or access to (or inability to use or access) the Visa Secure services; or
   (b) any other failure of performance, error, omission, interruption or defect, or any loss or delay in transmission or a transaction.
3. If you are dissatisfied with any aspect of the Visa Secure service, your sole and exclusive remedy is to terminate participation in the Visa Secure transaction or service, as provided in these Conditions of Use.

Section 28. Your conduct and visa secure

1. Whilst using the Visa Secure service and Our Internet banking services, you agree not to:
   (a) Impersonate any person or entity using the Visa Secure authentication process;
   (b) upload, post, email or otherwise transmit any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment used by the Visa Secure service or by us;
   (c) spam or flood our Internet banking service and the Visa Secure service;
   (d) modify, adapt, sub-license, translate, sell, reverse engineer, decompile or disassemble any portion of the Visa Secure service;
   (e) remove any copyright, trademark, or other proprietary rights notices contained in the Visa Secure service;
   (f) "frame" or "mirror" any part of the Visa Secure service without our prior written authorisation;
   (g) use any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index, "data mine," or in any way reproduce or circumvent the navigational structure or presentation of the Visa Secure service;
   (h) otherwise interfere with, or disrupt the Visa Secure service or our Internet banking services or servers or networks connected to us or the Visa Secure service or violate these Conditions of Use or any requirements, procedures, policies or regulations in relation to the Visa Secure service; or
   (i) intentionally or unintentionally violate any applicable local, state, national or international laws or regulations relevant or applicable to the Visa Secure service.

Section 29. Privacy and visa secure

1. We (or our nominated service provider) may collect personal information about you for the purposes of providing the Visa Secure service to you.
2. You authorise us to disclose personal information to others in order to execute your instructions including, but not limited to, conducting the Visa Secure service and investigating disputes or allegations of unauthorised transactions, or if it is required by law.
3. For more details of how your personal information is handled, please refer to our privacy policy, which can be viewed by accessing our Internet home site or you can obtain a copy by calling us.

Section 30. Click to Pay

1. This Section 30 applies to use of Click to Pay with your Visa Card even if you have previously self-enrolled the Visa Card for Click to Pay directly with Visa.
2. The other terms and conditions in these Conditions of Use applicable to use of your Visa Card still apply when using Click to Pay.
3. You must not misuse or interfere with Click to Pay.
4. Click to Pay uses your email address or mobile number to identify you and your linked cards. Click to Pay may automatically populate your billing address with the address you have provided to us. It is your responsibility to ensure the contact details you have provided to us are correct and remain up to date.
5. Visa may modify Click to Pay from time to time. Your continued use of Click to Pay indicates acceptance. We may update the terms and conditions applicable to Click to Pay in accordance with these Conditions of Use.
6. You may unenroll your Visa Card from Click to Pay at any time by contacting the bank.
7. Neither we nor Visa are a party to transactions between you and a merchant using Click to Pay.
8. Our Privacy Policy and Privacy Notice apply to our disclosure and use of your personal information in relation to Click to Pay.

Section 31. Regular Payment Arrangements

1. You should maintain a record of any regular payment arrangement that you have entered into with a Merchant.
2. To change or cancel any regular payment arrangement you should contact the merchant or us at least 15 days prior to the next scheduled payment. If possible, you should retain a copy of this change/cancellation request.
3. Should your card details be changed (for example if your Visa Card was lost, stolen or expired and has been replaced) then you must request the Merchant to change the details of your existing

regular payment arrangement to ensure payments under that arrangement continue. If you fail to do so your regular payment arrangement may not be honoured, or the merchant may stop providing the goods and/or services.

4. Should your Visa Card or your Accounts with us be closed for any reason, you should immediately contact the merchant to change or cancel your regular payment arrangement, as the merchant may stop providing the goods and/or services.

Section 32. MAKING AND RECEIVING NPP PAYMENTS USING PAYID

1. The PayID service is the NPP Payment addressing service that enables payers to make NPP Payments to payees using an alternative identifier instead of Account details.
2. Before you can create your PayID to receive NPP Payments into your Account, you have to satisfy us that you either own or are authorised to use your chosen PayID and you have an eligible Account.
3. Whether you choose to create a PayID for your Account or not, you and each Authorised User, may use a payee's PayID to make particular types of NPP Payments to the payee from your Account provided that:
   a) we and the payee's financial institution support the NPP Payment Service;
   b) the payee's Account is able to receive the particular NPP Payment; and
   c) the PayID is not locked.
4. You may create a PayID as long as it is a supported PayID Type. Some PayID Types, for example Organisation IDs, are restricted to business customers and organisations. Only eligible customers will be able to create a PayID that is a restricted PayID Type.
5. You must satisfy us that you own or are authorised to use your chosen PayID before you can use it to receive NPP Payments. This means we may ask you to provide evidence to establish this to our satisfaction, whether you are already registered for any other mobile or Internet banking or online payment services with us or not.
6. Depending on the policy of a payer's financial institution, your PayID Name may be displayed to payers who send NPP Payments to you. At the same time you create your PayID, we will either enable you to:
   a) Confirm your selection of a PayID Name for display to payers; or
   b) Select an alternative PayID Name, such as your business name, for display.
7. We will not permit selection of a PayID Name that is likely to mislead or deceive a payer into sending you NPP Payments intended for another payee, or for which for nay reason is appropriate.
8. We will not create a PayID for you without your prior consent.
9. You may choose to create more than one PayID for your Account.
10. If your Account is a joint Account, you and each other joint Account holder can create a unique PayID for the Account.
11. If you have authorised users on your Account, each authorised user may create a unique PayID for the Account.
12. Once a PayID is created and linked to your Account, it may not be used in relation to any other Account with us or with any other financial institution.
13. The PayID service does not support duplicate PayIDs. If you try to create a PayID for your Account which is identical to another PayID in the service, you will see the following message "Unable to Register PayID". You can contact us to discuss duplicate PayIDs. We cannot disclose details of any personal information in connection with duplicate PayIDs.
14. You can transfer your PayID to another Account with us, or to an Account with another financial institution by submitting a request to us.
15. A transfer of your PayID to another Account with us will generally be effective immediately, unless we notify you otherwise.
16. By creating your PayID you acknowledge that you authorise:
    a) us to record your PayID, PayID Name and Account details in the PayID service;
    b) NPP Participants which are payers' financial institutions will use your PayID information for the purposes of constructing NPP payment messages, enabling payers to make NPP Payments to you. We will disclose your PayID Name to payers for NPP Payment validation.
17. A transfer of your PayID to another financial institution is a two-step process initiated by you and completed by that financial institution. First, ask us to put your PayID into a transfer state and then complete the transfer via your new financial institution. Until the transfer is completed, NPP Payments to your PayID will be directed to your Account with us. If the other financial institution does not complete the transfer within 14 days, the transfer will be deemed to be ineffective and your PayID will remain with your Account with us. You can request transfer of your PayID at any time.

    Note: Transferring a PayID [to another financial institution] will cause payments under any PayTo Payment Agreement linked to that PayID to fail unless you also transfer the Payment Agreement: see Section 43.20 and Section 43.21.
18. A locked PayID cannot be transferred.
19. To transfer a PayID that you created for an Account with another financial institution to your Account with us, you will need to start the process with that financial institution.

    Note: If the PayID is linked to a PayTo Payment Agreement, the Payment Agreement will not automatically transfer with the PayID. You will need to take additional steps if you wish to transfer the Payment Agreement to your account with us: see Section 40.4.
20. You can close your PayID via internet banking, the Mobile Banking App or by calling us on 132 067.

    Note: Closing a PayID will cause payments under any PayTo Payment Agreement linked to that

PayID to fail unless you also transfer the Payment Agreement: see Section 43.20 and Section 43.21.

21. You must notify us immediately if you no longer own or have authority to use your PayID.
22. We monitor PayID use to manage PayID misuse and fraud. Your PayID will be locked if we reasonably suspect misuse of your PayID or use of your PayID to procure NPP Payments fraudulently.
23. You can request to unlock a locked PayID. The PayID will be unlocked when it has been confirmed that the PayID has not been misused.
24. Where we and the sending financial institution determine that an NPP Payment made to your Account is either a Mistaken Payment or a Misdirected Payment, we may, without your consent, and subject to complying with any other applicable terms and conditions, deduct from your Account, an amount up to the original amount of the Mistaken Payment or Misdirected Payment. We will notify you if this occurs.

Section 33. Using Osko®

1. You can make an Osko® payment which allows you to make everyday payments in a fast and versatile way.
2. Transaction limits may apply from time-to-time on the amount of Osko Payments that you can make. These transaction limits are set out in our *Fees and Charges* brochure
3. Money is transferred in near real-time with close to immediate funds availability, even if the individuals involved use different financial institutions or the payment is made over the weekend.
4. When you tell us to make an Osko payment you must tell us the bank account details or PayID of the person or business you wish to pay and the amount to be paid and the Account from which the amount is to be paid.
5. Not all Australian Accounts will be able to receive payments via the NPP. We will only effect your Osko payment if you give us all the specified information.
6. In order to make an Osko payment you do not have to have a registered PayID.
7. When you direct an Osko payment or a payment request to a PayID your full legal name and last known address as held by Regional Australia Bank will be provided to the receiving financial institution. This information will not be provided to the payment recipient and will be disposed of by the receiving financial institution in accordance with the Privacy Act (1998) (Cth).
8. When you direct an Osko payment or payment request to a PayID connected to a joint Account, other Account holders may be able to see the messages and notifications associated with the payment or payment request. Similarly, depending on the settings you choose for your PayID, other Account holders on your Account may be able to see messages and notifications associated with Payments and Payment Requests addressed to your PayID.

When initiating a Transaction, you might direct the Transaction to an incorrect Account if you get a PayID wrong. To try to avoid this, we will ask you to verify that you have the right PayID. We will do this by presenting you with the associated PayID Name as an additional confirmation of the intended recipient before you submit a transaction

Section 34. Processing Osko® Payments

1. We will attempt to make sure that your Osko payments are processed promptly by participants, and you must tell us promptly if:
   - you become aware of any delays or mistakes in processing your Osko payment;
   - you did not authorise an Osko payment that has been made from your Account; or
   - you think that you have been fraudulently induced to make an Osko payment.

   Please keep a record of the Osko receipt numbers on the relevant bills.
2. When you want us to send a payment direction you must give us the recipients PayID, their name, the amount of the transfer and the Account payment the transfer is to come from. You should ensure all information you provide in relation to an Osko payment is correct as an Osko payment instruction is irrevocable.
3. Except for scheduled or recurring payments, you cannot stop Osko payments once you have instructed us to make it and we cannot reverse it.
4. We will treat your Osko payment instruction as valid if, when you give it to us, you use the correct access method.
5. You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay) when making an Osko payment or if you did not authorise an Osko payment that has been made from your Account.

   Note: You must provide us with written consent addressed to the payee who received that Osko payment. If you do not give us that consent, the payee may not be permitted under law to disclose to us the information we need to investigate or rectify that Osko payment.
6. An Osko payment is treated as received by the payee to whom it is directed:
   - upon receipt of a successful payment notification approximately 15 seconds after the transfer has been submitted; and

     Note: An Osko payment may take longer to be credited to a payee if there is anything suspicious about the payment that requires investigation.
   - notwithstanding this, a delay may occur processing a Osko payment if a payee, or another financial institution participating in the NPP, does not comply with its Osko obligations.
7. You must be careful to ensure you tell us the correct amount you wish to pay. If you make a Osko payment and later discover that:
   - the amount you paid was greater than the amount you needed to pay - you must contact the payee to obtain a refund of the excess; or
   - the amount you paid was less than the amount you needed to pay - you can make another payment for the difference between the

amount you actually paid and the amount you needed to pay.

8. If you are responsible for a mistaken Osko payment and we cannot recover the amount from the person who received it within twenty (20) banking business days of us attempting to do so, you will be liable for that payment.
9. Please see our Fees and Charges brochure for current fees and charges in relation to Osko Payments.

Section 35. Scheduled and Recurring Osko® Payments

You may schedule Osko payments in advance of the time for payment as well as scheduling recurring Osko payments. If you use this option you should be aware of the following:

(a) you are responsible for maintaining, in the Account to be drawn on, sufficient cleared funds to cover all future-dated Osko payments (and any other drawings) on the day(s) you have nominated for payment or, if the Account is a credit facility, there must be sufficient available credit for that purpose;

(b) if there are insufficient cleared funds or, as relevant, insufficient available credit, the Osko payment will not be made and you may be charged a dishonour fee. Please refer to our Fees and Charges brochure.

(c) you are responsible for checking your Account transaction details or Account statement to ensure the future-dated payment is made correctly; and

(d) you should contact us if there are any problems with your future-dated payment.

Section 36. Authority to Recover Mistaken or Misdirected NPP Payments

Where we and the sending financial institution determine that an NPP Payment made to your Account is either a Mistaken Payment or a Misdirected Payment, we may, without your consent, deduct from your Account, an amount up to the original amount of the Mistaken Payment or Misdirected Payment. We will notify you if this occurs.

Section 37. Creating a PayTo Payment Agreement

1. PayTo allows you to establish and authorise Payment Agreements with merchants or Payment Initiators who offer PayTo as a payment option.
2. 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 that merchant or Payment Initiator with your personal information including your BSB and account number, or your PayID. You are responsible for ensuring the information you provide to the merchant or Payment Initiator is correct. Any personal information or data you provide to the merchant or Payment Initiator will be subject to their own privacy policy and terms and conditions.
3. Payment Agreements must be recorded in the Mandate Management Service before NPP Payments can 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 notify you of the creation of a Payment Agreement, and provide details of the merchant or Payment Initiator, 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 effective. If you decline, we will note that against the record of the Payment Agreement in the Mandate Management Service.
4. We will only process payment instructions in connection with a Payment Agreement once you have confirmed the Payment Agreement and it is effective. Once the Payment Agreement is effective we will process payment instructions received from the merchant's or Payment Initiator's financial institution. We are not liable for any loss you or any other person may suffer as a result of our processing a payment instruction submitted under a Payment Agreement that you have confirmed.

   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.
5. 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.
6. If you believe the payment amount or frequency or other detail presented is in 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.
7. This Section 37 does not apply to Migrated DDR Mandates.

Section 38. Amending a Payment Agreement

1. Your Payment Agreement may be amended by the merchant or Payment Initiator from time to time, or by us on your instruction.
2. We will notify you of proposed amendments to a Payment Agreement requested by the merchant or Payment Initiator. Such amendments may include variation of the payment amount (if a fixed amount) or payment frequency. 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 effective. If you decline, the amendment will not be made and the Payment Agreement will continue on existing terms.

3. If you do not confirm or decline an amendment request within 5 calendar days of it being sent to you, then the amendment request will be deemed to be declined.
4. 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.
5. Once an amendment request has been confirmed by you, we will promptly update the Mandate Management Service with this information.
6. Once a Payment Agreement has been established, you may instruct us to amend your name or transfer the Payment Agreement to another account you hold with us. If you wish to transfer the Payment Agreement to an account with another financial institution, you may give us a transfer instruction (see Section 4040 "Transferring your Payment Agreement"). 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.

Section 39. PAUSING YOUR PAYMENT AGREEMENT

1. You may instruct us to pause and resume your Payment Agreement. 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. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the pause or resumption. While the Payment Agreement is paused, we will not process payment instructions in connection with it. We are not liable for any loss that you or any other person may suffer as a result of you pausing a Payment Agreement.

   Before pausing a Payment Agreement you should ensure this will not breach, or result in a breach of, any contract you have with the merchant or Payment Initiator.
2. A merchant or Payment Initiator may pause and resume a Payment Agreement to which you are a party, in which case we will promptly notify you of that pause or subsequent resumption. We are not 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.

Section 40. TRANSFERRING YOUR PAYMENT AGREEMENT

1. When available, you may ask us to initiate the transfer of a Payment Agreement to an account at another financial institution. We will provide you with a Transfer ID to provide to your new financial institution to enable them to complete the transfer.
2. Your new financial institution will be responsible for obtaining your consent to transfer the Payment Agreement and for updating the Payment Agreement in the Mandate Management Service. The updated Payment Agreement will only become effective upon being updated in the Mandate Management Service.
3. Until the transfer is completed, the Payment Agreement will remain linked to your account with us and payments under the Payment Agreement will continue to be made from 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.
4. 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. We will use reasonable endeavours to process the transfer within 14 calendar days. Not 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.

Section 41. CANCELLING YOUR PAYMENT AGREEMENT

1. You may instruct us to cancel a Payment Agreement on your behalf. We will act on your instruction promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the cancellation. We are not liable for any loss that you or any other person may suffer as a result of cancelling a Payment Agreement.

   You may remain liable to the merchant or Payment Initiator for payments that would otherwise have been paid under the Payment Agreement, including for any cancellation fees.
2. A merchant or Payment Initiator may cancel a Payment Agreement to which you are a party, in which case we will promptly notify you of that cancellation. We are not liable for any loss that you or any other person may suffer as a result of cancellation of your Payment Agreement by the merchant or Payment Initiator.

Section 42. MIGRATION OF DIRECT DEBIT ARRANGEMENTS

1. A merchant or Payment Initiator who has an existing direct debit arrangement with you, may migrate it to a Payment Agreement, as a Migrated DDR Mandate. We are not obliged to notify you of a Migrated DDR Mandate. We will process instructions received from a merchant or Payment Initiator on the basis of a Migrated DDR Mandate.

   A Migrated DDR Mandate takes effect without your confirmation. If you do not consent to the migration of a direct debit arrangement you should contact the merchant or Payment Initiator.
2. A Migrated DDR Mandate has effect as a Payment Agreement. You may amend, pause (and resume), cancel or transfer your Migrated DDR Mandates, and will receive notice of amendment, pause or resumption, or cancellation initiated by the merchant or Payment Initiator of your Migrated

DDR Mandates, in the same manner as for other Payment Agreements.

Section 43. GENERAL PAYTO PROVISIONS

1. A Payment Agreement can only be linked to an account that has the PayTo facility.
2. You must carefully consider any Payment Agreement creation request, or amendment request made in respect of a Payment Agreement, and promptly respond to such requests. We are not 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.
3. You must notify us immediately if you no longer hold or have authority to operate the account from which a payment under a Payment Agreement has been or will be made.
4. You must promptly respond to any notification that you receive from us regarding the pausing or cancellation of a Payment Agreement for misuse, fraud or for any other reason. We are not responsible for any loss that you suffer as a result of you not promptly responding to such a notification.
5. You are responsible for complying with the terms of any agreement that you have with a merchant or Payment Initiator, including any termination notice periods. You are responsible for any loss that you suffer in connection with you cancelling or pausing a Payment Agreement, including for a breach of any agreement that you have with that merchant or Payment Initiator.
6. You are responsible for ensuring that you have sufficient funds in your account to meet the requirements of all your Payment Agreements. We are not responsible for any loss that you suffer as a result of your account having insufficient funds to meet a payment instruction under a Payment Agreement. See Overdrawing Account. for our rights if there are insufficient funds in your account.
7. 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 immediately.
8. From time to time we may ask you to confirm that your Payment Agreements are accurate and up to date. You must promptly respond to any such request. Failure to respond may result in us pausing the Payment Agreements.
9. We recommend that you allow notifications from the Mobile Banking App to your smartphone to ensure that you're able to receive and respond to Payment Agreement creation requests, amendment requests and other notifications in a timely way.
10. You are responsible for ensuring that: (i) all data you provide to us or to any merchant or Payment Initiator that subscribes to PayTo is accurate and up to date; (ii) you do not use PayTo to send threatening, harassing or offensive messages to the merchant, Payment Initiator or any other person; and (iii) any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.
11. All intellectual property, including but not limited to the PayTo trade marks 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 PayTo in a way that is consistent with these terms and conditions.
12. 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 PayTo or would have had the effect of removing functionality or adversely affecting the performance of PayTo); and (iv) your failure to use Our Intellectual Property in accordance with this agreement.
13. We may cancel or suspend your use of PayTo in accordance with our rights under Section 22 Cancellation of Visa Card or Of Access to Online Banking Services, BPAY or PayTo.
14. We may amend the terms and condition relating to PayTo in accordance with our rights under Notifying Changes. If you do not accept our amendments, you may cease using PayTo.
15. You must comply with all applicable laws in connection with your use of PayTo.
16. We will accurately reflect all information you provide to us in connection with a Payment Agreement in the Mandate Management Service.
17. We may monitor your Payment Agreements for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreements if we reasonably suspect misuse, fraud or security issues. We will promptly notify you of any such action.
18. If you become aware of a payment being made from your account, that is not permitted under the terms of your Payment Agreement or that was not authorised by you, contact us immediately and submit a claim. We will promptly respond to all claims and if the claim is founded, we will refund your account. We are not liable to you for any payment made that was in fact authorised by the terms of your Payment Agreement.
19. We may impose daily, or other periodic, limits on the value of payments that can be made using PayTo. These limits are set out in the *Fees and Charges* brochure. We may reject any payment instructions from a merchant or Payment Initiator that will cause you to exceed any such limit. We are not liable for any loss that you or any other

person may suffer as a result of us rejecting a payment instruction under this clause.

20. If your Payment Agreement is linked to a PayID:
    (a) transferring your PayID to another [financial institution]/[account (whether with us or another financial institution)] will not automatically transfer the Payment Agreement to that [financial institution]/[account], and payments under the linked Payment Agreement will fail (subject to Section 43.21);
    (b) closing your PayID will cause payments under the linked Payment Agreement to fail (subject to Section 43.21).
21. To ensure payments under a linked Payment Agreement continue after transferring or closing the PayID you will also need to either link the Payment Agreement to an account with us (see Section 388 "Amending a Payment Agreement") or transfer the Payment Agreement to another financial institution (see Section 4040 "Transferring your Payment Agreement").

Section 44. PRIVACY AND PAYTO

By confirming a Payment Agreement or permitting the creation of a Migrated DDR Mandate against your account with us, you acknowledge that you authorise us to collect, use and store your personal information and the details of your Payment Agreement or Migrated DDR Mandate in the Mandate Management Service, and that these details may be disclosed to the financial institution or payment processor for the merchant or Payment Initiator, for the purposes of creating payment instructions and constructing NPP Payment messages and enabling us to make payments from your account.

Section 45. AUTHORITY FOR PAYTO INSTRUCTIONS

Your instructions in relation to a Payment Agreement must be provided in accordance with the account operating instructions for the account that is, or is intended to be, linked to the Payment Agreement. This includes instructions to confirm or decline a Payment Agreement or the merchant's or Payment Initiator's amendments to a Payment Agreement, or to amend, pause, resume, cancel or transfer a Payment Agreement. For example, instructions to confirm a Payment Agreement linked to a joint account operated on an 'all to sign' basis must be provided by all the joint holders.

Section 46. CONFIRMATION OF PAYEE

Confirmation of Payee service

1.1 Confirmation of Payee is a service that applies when sending money to an account using BSB and account number. It is designed to help payers avoid scams or mistaken payments.

1.2 The Confirmation of Payee service matches the account details entered (which must also include an account name) with the account details held by the recipient's financial institution and displays the outcome, which could be a match, a close match or a no match.

1.3 If the intended recipient is a business or other organisation, or the outcome is a match or close match, then the account name will be displayed to the payer.

Conducting a Confirmation of Payee lookup

1.4 When making a payment from your account using BSB and account number it is the user's responsibility to ensure they provide the correct BSB and account number.

1.5 The Confirmation of Payee service will provide the user with a match, a close match or a no match outcome. If the user thinks the account details were entered incorrectly, they can check them again before making the payment. If something does not seem right, the user should check the account details with the intended recipient before proceeding, or choose not to proceed with the payment.

1.6 You must not use, and must ensure any other user does not use, the Confirmation of Payee service other than for its intended purpose, or in breach of these Conditions of Use. We may limit or suspend use of the Confirmation of Payee service from your account if we believe it reasonably necessary to protect you, us or a third party from possible fraudulent activity, scams or other activity that may cause loss or damage.

1.7 We are not responsible for the accuracy of the recipient's account details provided to us from the recipient's financial institution.

Use and disclosure of your account details

1.8 You authorise, and provide consent to:
    (a) us to use, store and disclose your account details in the Confirmation of Payee service; and
    (b) payers' financial institutions to use and disclose your account details for the purposes of the Confirmation of Payee service and prior to making payments to you.

1.9 In special circumstances we may allow you to opt-out of the Confirmation of Payee service. Please contact us.

1.10 However, even if you do opt-out of the service, we will still confirm, disclose, store and use your account details through the Confirmation of Payee service for use by government agencies for the purposes of making a payment to you.

1.11 In some circumstances you may provide alternative names to be recorded on your account for use in the Confirmation of Payee service. Please contact us.

Section 47. MISUSE OF PAYMENT DESCRIPTION AND TRANSACTION MESSAGING

Purpose of payment text fields

Payment descriptions, references and any other free-text fields in payments (including NPP payments such as PayID and Osko, and any other payment channels we offer) are provided to help identify a payment. They must not be used to communicate messages unrelated to the payment.

Prohibited content and conduct

You must not use your account, our services, or any payment text field to engage in conduct that we reasonably consider:

1. Is unlawful;

2. Is used as a vehicle for, or may cause or result in financial abuse, coercive control, stalking, harassment, intimidation, or threats;
3. Is offensive, defamatory, discriminatory, harassing, or threatening to any person;
4. Promotes or encourages physical or psychological harm to nay person, self-harm, violence, or terrorism;
5. Includes or facilities serious criminal communication (including content relating to child exploitation or child abuse material); OR
6. Includes confidential information, sensitive personal information about any person, or content that is otherwise inappropriate for a payment description/reference.

Our rights and actions

If we reasonably suspect a breach of this section or other misuse of payment text fields, we may (to the extent permitted by law and without notice where appropriate):

- Decline, delay, block, or reverse the relevant payment or other transaction;
- Restrict your access to certain payment features or channels (including electronic banking);
- Impose conditions on your use of the account;
- Issue warnings (including written warnings) and require undertakings that the behaviour will stop;
- Suspend or close your account(s) or end our banking relationship with you; and
- Report matters to relevant authorities and share information with other financial institutions or payment system participants where required or permitted by law, including for AML/CTF purposes.

Support for customers experiencing abuse

If you are receiving abusive or threatening payment messages, or you are experiencing financial abuse, you can contact us when it is safe to do so. We can discuss options to improve your banking safety (which may include account changes and additional safeguards).

Section 48. INFORMATION SHARING (INCLUDING PERSONAL INFORMATION)

We may report matters to relevant authorities and share information (including personal information and transaction details) with other financial institutions, payment system participants and relevant service providers where required or permitted by law, including to help prevent, detect, investigate and respond to scams (including under the Scams Prevention Framework), fraud, financial abuse, money laundering, terrorism financing and child exploitation. We handle personal information in accordance with our privacy policy. Where permitted by law, we may do this without notifying you (for example, to avoid prejudicing investigations or protective action).

ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE

Customer owned banking delivers Member and Customer focused, competitive services. Mutual Banks are customer-owned financial institutions committed to putting their Members and Customers first. The Customer Owned Banking Code of Practice, the code of practice for customer owned banks, is an important public expression of the value we place on improving the financial wellbeing of our individual Members, Customers and their communities.

Our Key Promises to you are

1. We will deliver banking services in the interests of our Members and Customers.
2. We will obey the law.
3. Will not mislead or deceive.
4. We will act honestly and fairly.
5. We will offer products and services that are fit for general purpose.
6. We will deliver services with reasonable care and skill.
7. We will contribute to our community.

You can download a copy of the Customer Owned Banking Code of Practice here

www.customerownedbanking.asn.au/consumers/cobcop

If you have a complaint about our compliance with the Customer Owned Banking Code of Practice you can contact

Code Compliance Committee Mutuals

PO Box 14240 Melbourne VIC 8001

Phone: 1300 78 08 08 Fax: 03 9613 7481

info@codecompliance.org.au

The Code Compliance Committee (CCC) is an independent committee, established in accordance with the Code, to ensure that subscribers to the Code are meeting the standards of good practice that they promised to achieve when they signed up to the Code. The CCC investigates complaints that the Code has been breached and monitors compliance with the Code through mystery shopping, surveys, compliance visits and complaint handling.

Please be aware that the CCC is not a dispute resolution body. To make a claim for financial compensation we recommend you contact us first. You can contact our external dispute resolution provider, the Australian Financial Complaints Authority, directly. However, they will refer the complaint back to us to see if we can resolve it directly with you before involving them.

You can contact the Australian Financial Complaints Authority:

by calling 1800 931 678

by visiting http://www.afca.org.au

by email info@afca.org.au

In writing GPO Box 3, Melbourne VIC 3001

13 October 2026

Head Office
Technology Park, Madgwick Drive, Armidale NSW 2350
PO Box U631, University of New England NSW 2351
Telephone 132 067 **Email** enquiries@regionalaustraliabank.com.au
Web regionalaustraliabank.com.au