Account & Access Facility
Conditions of Use

THIS DOCUMENT MUST BE READ TOGETHER WITH:

Summary of Accounts and Availability of Access Facilities Brochure, Fees and Charges and Transaction Limits Brochure.

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

Date taking effect: 8 August 2016

The Regional Australia Bank Account and Access Facility is issued by:
Regional Australia Bank Ltd
ABN 21 087 650 360
Australian Financial Services 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
- Fax us on 02 6776 0430

To report the loss, theft or unauthorised use of your Visa card

- **in Australia**
  call the Visa card Hotline on 1800 139 241 or 02 9959 7530, 24 hours a day, everyday. Please also contact us to report the loss, theft or unauthorised use.
- **overseas – for Visa**
  Please contact us before you travel overseas for the current Visa hotline arrangements

To report the loss, theft or unauthorised use of your Regional Australia Bank Access Card

- **in Australia**
  call Regional Australia Bank on 132 067 the First Data Hotline on 1800 139 241 or 02 9959 7530.
- **Overseas**

Call Regional Australia Bank on +61 2 6776 6400 or the First Data Hotline on +61 2 9959 7530. Please contact us before you travel overseas for the current Visa hotline arrangements

To report the loss of any other access facility, or any other unauthorised transaction, contact us as set out above in How to Contact Us.

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 and Transaction Limits 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.

ACCOUNT OPERATIONS

WHAT IS THE REGIONAL AUSTRALIA BANK ACCOUNT AND ACCESS FACILITY?

The Regional Australia Bank Account and Access Facility is a facility that gives you transaction, savings and term savings accounts as well as these facilities for accessing accounts:

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

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 methods attaching to each account type.

HOW DO I OPEN AN ACCOUNT?

You will need to become a member of Regional Australia Bank before we can issue the Regional Australia Bank Account and Access Facility to you. To become a member, you will need to:

- complete a membership application form; and
- subscribe for a member share in Regional Australia Bank.

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 we issue you with the Regional Australia Bank Account and Access Facility, you have access to the S1 Access Savings 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.

WHAT FEES AND CHARGES ARE THERE?

Please refer to the *Fees & Charges and Transaction Limits* 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.

WHAT INTEREST CAN I EARN ON MY ACCOUNT?

Our Interest Rates brochure provides information about our current deposit and savings interest rates. Our website also has information about our current deposit and savings interest rates. We may vary deposit or savings interest rates from time to time on all deposit accounts except our term deposit accounts.

Our *Summary of Accounts & Availability of Access Facilities* brochure discloses how we calculate and credit 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 (TFN)

When you apply for the Regional Australia Bank Account and Access Facility we will ask you whether you want to disclose your Tax File Number or exemption. If you disclose it, we will note your TFN against any account you activate.

You do not have to disclose your TFN to us. If you do not, we are required to deduct general withholding tax, on behalf of the Australian Taxation Office, from interest paid on the account at the highest marginal rate.

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.

Businesses need only quote their ABN instead of a TFN.

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 under the Regional Australia Bank Account & Access Facility 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.

You may revoke the authorised person's authority at any time by giving us written notice.

MAKING DEPOSITS TO THE ACCOUNT

You can make deposits to the 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
- by cash or cheque at an ANZ Bank branch using a specially encoded deposit book
- via Australia Post Bank@Post.

Note that electronic deposits may not be processed on the same day. Please refer to EFT Co*nditions of Use: Section 8,* on page 8.

DEPOSITING CHEQUES DRAWN ON AUSTRALIAN BANKS

You can only access the proceeds of a cheque when it has cleared. This usually takes 3 business days. However, you can ask us for a special clearance for which we may charge a fee. Please refer to our *Fees & Charges and Transaction Limits* brochure for our current fee for special clearances.

WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT

You can make withdrawals from the account:

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

unless otherwise indicated in the *Summary of Accounts & Availability of Access Facilities* brochure.

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.

DEBITING TRANSACTIONS GENERALLY

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

OVER THE COUNTER WITHDRAWALS

Generally, you can make over-the-counter withdrawals in cash or by buying a Regional Australia Bank Corporate Cheque. Please check:

- the *Summary of Accounts & Availability of Access Facilities* brochure for any restrictions on withdrawals applying to certain accounts;
- the *Fees & Charges and Transaction Limits* brochure for any applicable daily cash withdrawal limits or other transaction limits.

WITHDRAWALS USING OUR BANK CHEQUES

This is a cheque Regional Australia Bank draws payable to the person you nominate. You can purchase a Corporate Cheque from us for a fee: see the *Fees & Charges and Transaction Limits* brochure.

If a corporate cheque is lost or stolen, you can ask us to stop payment on it. You will need to complete a form of request, giving us evidence of the loss or theft of the cheque. You will also have to give us an indemnity – the indemnity protects us if someone else claims that you wrongfully authorised us to stop the cheque.

We cannot stop payment on our corporate 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 & Charges and Transaction Limits* brochure.

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 to zero for security reasons.

OVERDRAWING AN ACCOUNT

You must keep sufficient cleared funds in your account to cover your cheque, direct debit and EFT transactions. If you do not, we can dishonour the transaction and charge dishonour fees: see the *Fees & Charges and Transaction Limits* brochure.

Alternatively, we can honour the transaction and overdraw your account. We will 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: see the *Fees & Charges and Transaction Limits* brochure.

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

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. You can ask us for an account statement at any time. We may charge a fee for providing additional statements or copies: see the *Fees & Charges and Transaction Limits* brochure.

We may also provide your statements electronically. Please ask us about this facility.

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?

We recommend that if you change your name or address, you let us know immediately.

Inactive Accounts

If no transactions are carried out on your account during each consecutive 12 month period (other than transactions initiated by Regional Australia Bank, 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 we will treat your account as being inactive.

Once your account becomes inactive, and in each consecutive 12 month period that your account remains inactive, we will charge an inactive fee. This fee is shown in the Fees and Charges brochure.

If your account remains inactive for seven (7) years, we have a legal obligation to remit balances exceeding $500 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 deposit account in the same name which is overdrawn.

On termination of your membership, 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 Centrelink 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 and Cancelling Access Facilities

You can close the Regional Australia Bank Account and Access Facility on request at any time. However, you will have to surrender your member cheque book and any access card at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding cheque, EFT transactions and fees, if applicable.

We can:

- close the Regional Australia Bank Account and Access Facility in our absolute discretion by giving you at least 14 days notice and paying you the balance of your account; or
- cancel any access facility for security reasons or if you breach these Conditions of Use.

Notifying Changes

We may change fees, charges, interest rates and other conditions at any time. 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
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
Changing any other term or condition	when we next communicate with you

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;
- notification on our website.

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

How We Send Notices & Statements

We may send you notices and statements:

- by post, to the address recorded in our membership records or to a mailing address you nominate;
- by email;
- by advertisement in the media, for some notices only.

If you agree, we may, instead of sending you a notice or statement, post notices or statements 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 the Regional Australia Bank Account and Access Facility or transactions on your account. 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.

If you want to make a complaint, contact our staff at any branch and tell them that you want to make a complaint. Our staff have a duty to deal with your complaint under our dispute resolution policy. 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 to you on request.

MEMBER CHEQUING

Member chequing allows you to make payments by cheque. We will issue you with a cheque book and authorise you to draw cheques on our account at the ANZ or another Bank as we chose. We will debit your account for the value of cheques you draw.

If you have insufficient funds in your nominated account we may instruct the Bank to dishonour your cheque. However, we have discretion to allow the cheque to be paid and to overdraw your account for this purpose. If you overdraw your account, we will charge you interest and fees. Please refer to the section Overdrawing an Account on page 2.

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

DIRECT DEBIT

You can authorise a participating biller to debit amounts from your account, as and when you owe those amounts to the biller. The biller will provide you with a Direct Debit Request (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 debit card, please contact us directly about unauthorised or irregular debits.

We can cancel your direct debit facility, in our absolute discretion, if three (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.

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 direct debit arrangement 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 direct debit arrangement 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 below to protect against unauthorised use of your access 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 Before Using a Device to Make Electronic Payments

- Sign the access card as soon as you receive it.
- Familiarise yourself with your obligations to keep your access card and pass codes secure.
- Familiarise yourself with the steps you have to take to report loss or theft of your access card or to report unauthorised use of your access card, BPAY® or 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.
- Never write the pass code on the access card.
- Never write the pass code PIN on anything which is kept with or near the access card.
- Never lend the access card to anybody.
- Never tell or show the 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 access card, access facility and pass codes you may increase your liability for unauthorised transaction.

Our epayments access facilities are:

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

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 & Charges and Transaction Limits* brochure for fees and charges in relation to EFT access facilities and transactions.

The ePayments Conditions of Use govern all ePayments transactions made using any one of our ePayments access facilities, listed above.

ACCESS CARD

Regional Australia Bank's Access Card allows you to access your account at an ATM or EFTPOS terminal in Australia. We will provide you with a PIN to use with your Access Card. Your Access Card allows you to:

- check your account balances;
- withdraw cash from your account.

Your Regional Australia Bank Access Card also allows you to access your account at an ATM or EFTPOS terminal overseas displaying the ***Visa / Plus logo***.

We may choose not to give you an Access Card if you are under 16.

VISA CARD

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. Visa Card also allows you to:

- check your account balances;
- withdraw cash from your account;
- transfer money between accounts
- deposit cash or cheques 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 18 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 EFT Transactions. Liability for such transactions will be determined in accordance with section 16 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 Electronic Equipment;
- 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.

CHARGEBACKS FOR VISA CARD

If a Visa Card transaction:

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

then you can ask us to 'chargeback' 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 Verified by Visa unless we are liable as provided in the EFT Conditions of Use.

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

BPAY®

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

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 Regional Australia Bank account, all you need is a Regional Australia Bank Access Card or Visa Debit Card which you can use with an accompanying Personal Identification Number (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:

(i) **"account"** means your account with us;

(ii) **"access method"** means a method we authorise for you to use as evidence of your authority to make an EFT 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 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 or Access Card - your Visa Card or Access Card and PIN used at an EFT terminal;

(iii) **"ATM"** means automatice teller machine;

(iv) **"authorised user"** means you and any peson you have considered to operate your account;

(v) **"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;

(vi) **"business day"** means any day on which we are open for business;

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

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

(i) ATM card;

(ii) Debit card or credit card; and

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

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

(x) **facility** means an arrangement through which you can perform transactions;

(xi) **identifier** means information that a user:

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

(ii) must provide to perform a transaction;

Examples include a member number or customer number

(xii) **"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 or Access Card and PIN to conduct an EFT transaction, for example, an automatic teller machine (ATM) or point of sale terminal (EFTPOS);

(xiii) **"ePayments transaction"** means an electronic funds transfer to or from your account using an access method and includes transactions carried out by means of:

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

(xiv) **"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;

(xv) **"internet site"** means our site at:

regionalaustraliabank.com.au

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

(xvii) **"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 PBay or PayID service;

(xviii) **"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;

(xix) **"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®;

(xx) **"NPP"** means the New Payments Platform operated by NPP Australia Limited.

(xxi) **"NPP Payments"** means payments cleared and settled via the NPP;

(xxii) **"Online Banking Services"** is the term used to encompass phone banking, internet banking, mobile banking and the mobile banking app;

(xxiii) **"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]

(xxiv) **"Osko"** leverages PayID to make payment via an easy to remember identifier.

(xxv) **"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).

(xxvi) **"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;

(xxvii) **"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.

(xxviii) **"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;

(xxix) **"transactiopn"** means a transaction to which these ePayment Conditions of Use apply;

(xxx) **"unauthorised transaction"** means a transaction that is not authorised by a user

(xxxi) **"user"** means you or an individual you have authorised to perform transactions on your account, including:

(i) a third party signatory to your account; and

(ii) a person you authorise us to issue an additional card to;

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

(xxxiii) "**you**" means:

- the person or persons 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 or Access Card to.

Section 3. SECURITY OF CARDS AND PASS CODES

1. The security of your access cards and pass codes is very important because they give unrestricted access to your account. You must take every effort to protect the card or pass codes from theft, loss or unauthorised use, to help to prevent fraudulent or unauthorised use of the access method.
2. You must not tell or show the pass code to another person.
3. You must take care to prevent another person, including your family and friends, from seeing you enter your pass code.
4. You must not select a pass code that represents your birth date or a recognisable part of your name. If you do use an obvious pass code, such as a name or date, you may be liable for any losses which occur as a result of unauthorised use of the pass code before you notify us that the pass code has been misused or has become known to someone else.
5. You must not record the pass code on any other part of your access method or keep a record of the pass code on anything which is kept with or near any other part of your access method unless reasonable steps have been taken to carefully disguise the pass code or to prevent unauthorised access to that record.
6. You must not act with extreme carelessness in failing to protect the security of the pass code.
7. Failure to adhere to these security requirements may render you liable for any financial loss.

Section 4. TRANSACTIONS

1. The ePayment Conditions of Use apply to payment, funds transfer and cash withdrawal transactions that are:
   (i) initiated using electronic equipment, and
   (ii) 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 mobile devices; and

(viii) Osko Payments.

Section 5. How To Report Loss, Theft Or Unauthorised Use Of Your Card or Pass Code

1. If you believe your Visa Card or Access 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 the Visa Card or Access Card Hotline at any time.

   Please refer to How to Contact Us on page 1 for our contact details.

2. If you believe your Token has been misused, lost or stolen you must immediately contact us during business hours.

   Please refer to How to Contact Us on page 1 for our contact details.

3. You must provide the following information when notifying us or the Visa Card or Access Card Hotline:
   - the Visa Card or Access 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 or Access Card .
4. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.
5. After contacting the Visa Card or Access Card Hotline, you should confirm the loss or theft as soon as possible at our office.
6. The Visa Card or Access Card Hotline is available 24 hours a day, 7 days a week.
7. If the Visa Card or Access Card Hotline is not operating when you attempt notification, nevertheless, 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 or Access 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.
8. 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 priority paid mail as soon as possible; or
   (ii) by telephoning the VISA Card Hotline number for the country you are in

VISA CARD HOTLINE

Australia wide toll free

1800 139 241 Sydney Metropolitan Area

02 9959 7530

ACCESS CARD HOTLINE

Australia wide toll free

1800 139 241Sydney Metropolitan Area

02 9959 7530 From Overseas

+61 2 9959 7530

Section 6. How to Report Unauthorised Use Of Online Banking Services

1. If you believe that your access method used for BPAY® or any other banking transactions, or any part of your access method, has been misused, lost or stolen, or, where relevant, your pass code has become known to someone else, you must contact us immediately.

   Please refer to How to Contact Us on page 1 for our contact details. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.

2. If you believe an unauthorised transaction has been made, including BPAY®, and your access method uses a pass code, you should change that pass code immediately.

Section 7. 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 & Charges and Transaction Limits* brochure.

   Please note that merchants, billers or other financial institutions may impose additional restrictions on the amount of funds that you can withdraw, pay or transfer.

2. We may also require you to apply for new transaction limits if you change any password or secret code in an access method. We will require you to provide proof of identity that satisfies us. We may reduce transaction limits to zero for security reasons.

Section 8. 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 9. 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 hours 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.
   - the Mobile Banking App, you must ensure that you log off from the Mobile Banking App.
6. Regional Australia Bank 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, Regional Australia Bank 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, tranfers, loan repayments and cheque withdrawals.

Section 10. MISTAKEN INTERNET PAYMENTS

1. In this section:
   (i) **"direct entry**" means a direct debit or direct credit;
   (ii) **"mistaken internet payment"** means a payment by a user through a 'Pay Anyone' internet banking facility and processed by an ADI through direct entry 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:
   (a) the user's error, or
   (b) the user being advised of the wrong BSB number and/or identifier.

   This does not include payments made using BPAY.
   (iii) **"receiving ADI"** means an ADI whose customer has received an internet payment;
   (iv) **"unintended recipient"** means the recipoient 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:
   (i) acknowledge the request by the sending ADI for the return of funds, and
   (ii) 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 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 4.2-Section 4.5, 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 11. USING BPAY®

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 12. 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.

   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 12.9) when making a BPAY® payment or if you did not authorise a BPAY® payment that has been made from your account.

   Please note that 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.

   Please note that the 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. Notwithstanding this, 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 banking business days of us attempting to do so, you will be liable for that payment.

Section 13. Future-Dated BPAY® Payments

Please note that this is an optional facility depending on whether we offer it.

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.
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 14. 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 15. Using Visa Card or Access Card

1. You agree to sign the Visa Card or Access Card immediately upon receiving it and before using it as a means of preventing fraudulent or unauthorised use of the Visa Card or Access Card. You must ensure that any other cardholder you authorise also signs their Visa Card or Access 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 or Access 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 & Charges and Transaction Limits brochure for details of current transaction limits Also note Section 7 that sets out how we can vary daily withdrawal limits from time to time.
4. You may only use your Visa Card or Access Card to perform transactions on those accounts we permit. We will advise you of the accounts which you may use your Visa Card or Access Card to access.
5. The Visa Card or Access Card always remains our property.

Section 16. USING VISA OR ACCESS 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 the Visa Card or Access 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 the Visa Card or Access Card are subject to a conversion fee. Please refer to the *Fees & Charges and Transaction Limits* 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. Before travelling overseas, you should obtain the Visa Worldwide card HOTLINE number for your country of destination as well as the Access Card Plus HOTLINE number from us.

Section 17. ADDITIONAL VISA CARD OR ACCESS CARD

1. You may authorise us, if we agree, to issue an additional Visa Card or Access Card to an additional cardholder provided this person is over the age of 18 (unless we agree to a younger age).
2. You will be liable for all transactions carried out by this cardholder.
3. We will give each additional cardholder a separate passcode.
4. You must ensure that any additional cardholders protect their Visa Card or Access Card and passcode in the same way as these ePayments Conditions of Use require you to protect your Visa Card or Access Card and passcode.
5. To cancel the additional Visa Card or Access Card you must notify us in writing. However, this cancellation may not be effective until the additional Visa Card or Access Card is returned to us or you have taken all reasonable steps to have the additional Visa Card or Access Card returned to us.
6. You may not be liable for the continued use of the additional Visa Card or Access Card from the date that you have:
   - notified us that you want it cancelled; and
   - taken all reasonable steps to have the additional Visa Card or Access Card returned to us.

   Please note that if you are unable to return the additional Visa Card or Access Card to us, we may require you to make a written statement describing the steps you have taken to return the card.

Section 18. USING VISA CARD OR ACCESS CARD TO MAKE DEPOSITS AT EPAYMENT TERMINALS

1. This Section only applies to deposits made at ePayments terminals using your Visa Card or Access Card.
2. Any deposit you make at an EFT terminal will not be available for you to draw against until your deposit has been verified by the EFT 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 EFT 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 EFT terminal (subject to our verification of the amount you deposit).

Section 19. USE AFTER CANCELLATION OR EXPIRY OF THE VISA CARD OR ACCESS CARD

1. You must not use your Visa Card or Access Card:
   (a) before the valid date or after the expiration date shown on the face of the Visa Card or Access Card; or
   (b) after the Visa Card or Access 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 20. EXCLUSIONS OF VISA CARD OR ACCESS CARD WARRANTIES AND REPRESENTATIONS

1. We do not warrant that merchants, ePayments terminals or ATMs displaying Visa Card or Access Card signs or promotional material will accept the Visa Card or Access Card.

2. We do not accept any responsibility should a merchant, bank or other institution displaying Visa Card or Access Card signs or promotional material, refuse to accept or honour the Visa Card or Access 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 21. 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 or Access 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 5 or Section 6 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 3; 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 21(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 22. 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.
2. 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 23. CANCELLATION OF VISA CARD OR ACCESS CARD OR OF ACCESS TO ONLINE BANKING SERVICES OR BPAY®

1. You may cancel your Visa Card or Access Card, your access to phone banking, internet banking, the Mobile Banking App, BPAY® or Osko® at any time by giving us written notice.
2. We may immediately cancel or suspend your Visa Card or Access 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) 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) if we cease to be a participant in Osko;
   (f) in the case of Visa Card or Access Card, we may cancel the Visa Card or Access Card by capture of the Visa Card or Access Card at any ePayments terminal or ATM.
3. We may cancel your Visa Card or Access Card or your access to phone banking, internet banking (including the Mobile Banking App), BPAY® or Osko 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 or Access Card, you will be liable for any transactions you make using your Visa Card or Access Card before the Visa Card or Access Card is cancelled but which are not posted to your account until after cancellation of the Visa Card or Access Card.
5. In the case of phone banking, internet banking (including the Mobile Banking App), BPAY® or Osko if, despite the cancellation of your access to phone banking, internet banking (including the Mobile Banking App), BPAY® or Osko you carry out a transaction using the relevant access method, you will remain liable for that transaction.
6. Your Visa Card or Access Card or your access to phone banking, internet banking (including the Mobile Banking App), BPAY® or Osko will be terminated when:
   (a) we notify you that we have cancelled your Visa Card or Access 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 or Access Card applies or which has phone banking, internet banking (including the Mobile Banking App), BPAY® or Osko access;
   (c) you cease to be our member; or
   (d) you alter the authorities governing the use of your account or accounts to which the Visa Card or Access Card applies or which has phone banking, internet banking (including the Mobile Banking App), BPAY® or Osko access (unless we agree otherwise).
7. In the case of Visa Card or Access Card, we may demand the return or destruction of any cancelled Visa Card or Access Card.

Section 24. 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 25. 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 chossed 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 chose 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.
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.
20. To close your PayID, go to www.regionalaustraliabank.com.au, log in to Internet banking and go to Settings.
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 eigher a Mistaken Payment or a Misdirected Payment, we may, withour 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 26. 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 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 New Payments Platform. 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 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 27. 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.

   Please note that 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

     Please note that the 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 ayment 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 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 28. 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;

(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 29. AUTHORITY TO RECOVER MISTAKEN OR MISDIRECTED 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.

ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE

Customer owned banking delivers member-focused, competitive services. Mutual Banks are customer-owned financial institutions committed to putting their members 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 and their communities.

Our 10 Key Promises to you are

1. We will be fair and ethical in our dealings with you
2. We will focus on our members
3. We will give you clear information about our products and services
4. We will be responsible lenders
5. We will deliver high customer service and

standards

6. We will deal fairly with any complaints
7. We will recognise member rights as owners
8. We will comply with our legal and industry obligations
9. We will recognise our impact on the wider community
10. We will support and promote this Code of Practice.

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
http://www.cobccc.org.au/for-consumers/before-you-report-a-concern/

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 Financial Ombudsman Service, 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 Financial Ombudsman Service:

by calling 1300 78 08 08

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

May 2018

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